SAINTwriter Exploit Report

Report Generated: December 14, 2015

1 Introduction

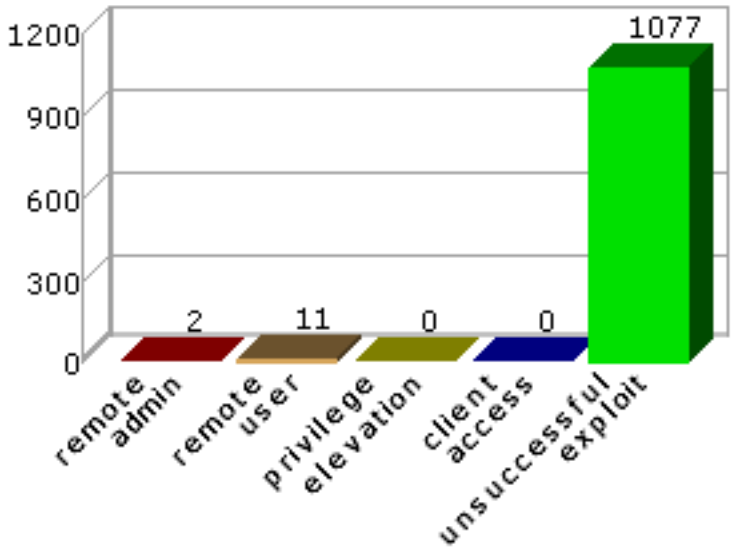
On December 14, 2015, at 12:50 PM, a Single Penetration scan was conducted using the SAINTexploit 8.9.28 exploit tool. The scan discovered a total of eight live hosts, and successfully performed two administrative level exploits, 11 user level exploits, zero privilege elevation exploits, and zero client access exploits. The hosts and problems detected are discussed in greater detail in the following sections.

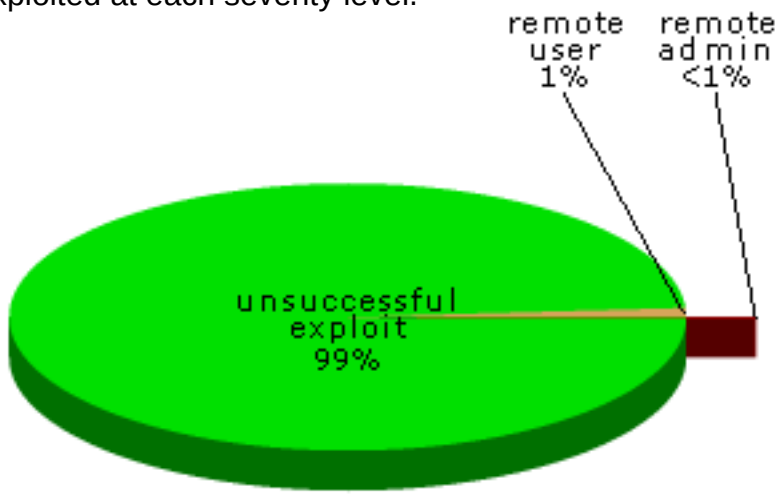
2 Summary

The sections below summarize the results of the scan.

2.1 Exploited Vulnerabilities by Severity

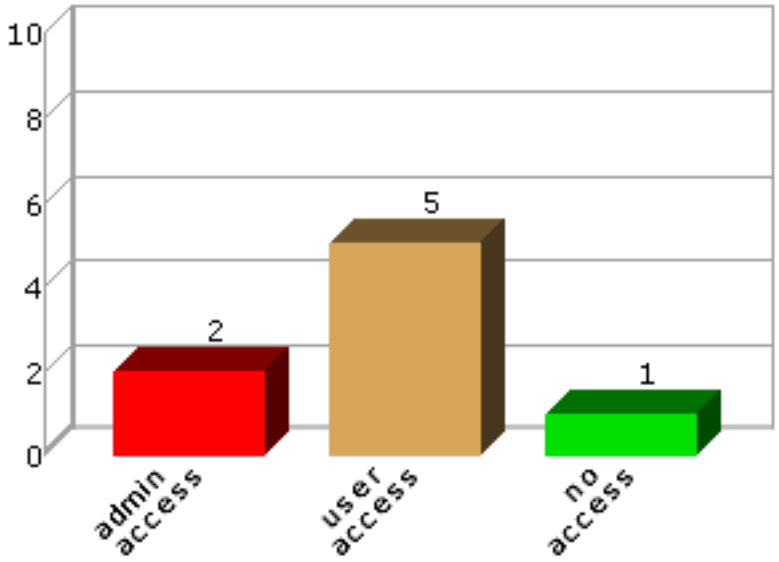
This section shows the overall number of vulnerabilities exploited at each severity level.

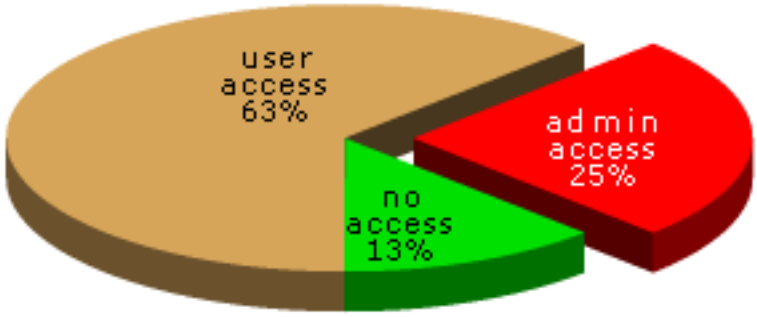




2.2 Exploited Hosts by Severity

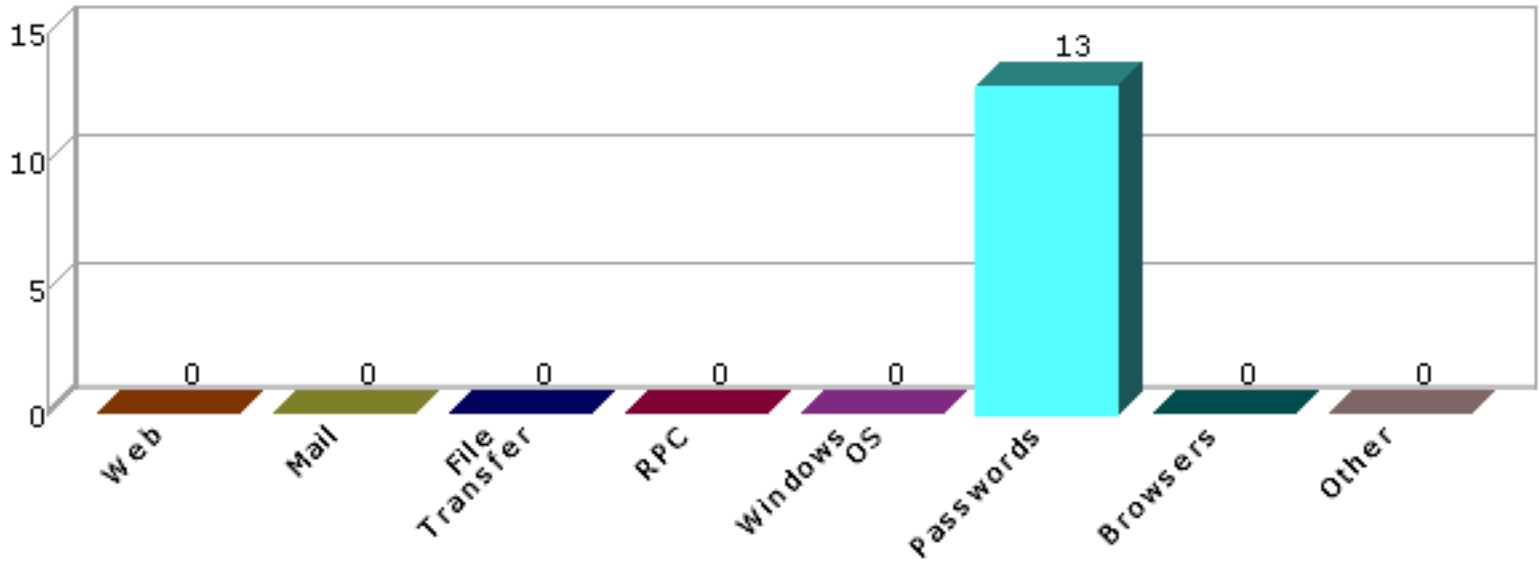
This section shows the overall number of hosts exploited at each severity level. The severity level of a host is defined as the highest vulnerability severity level exploited on that host.

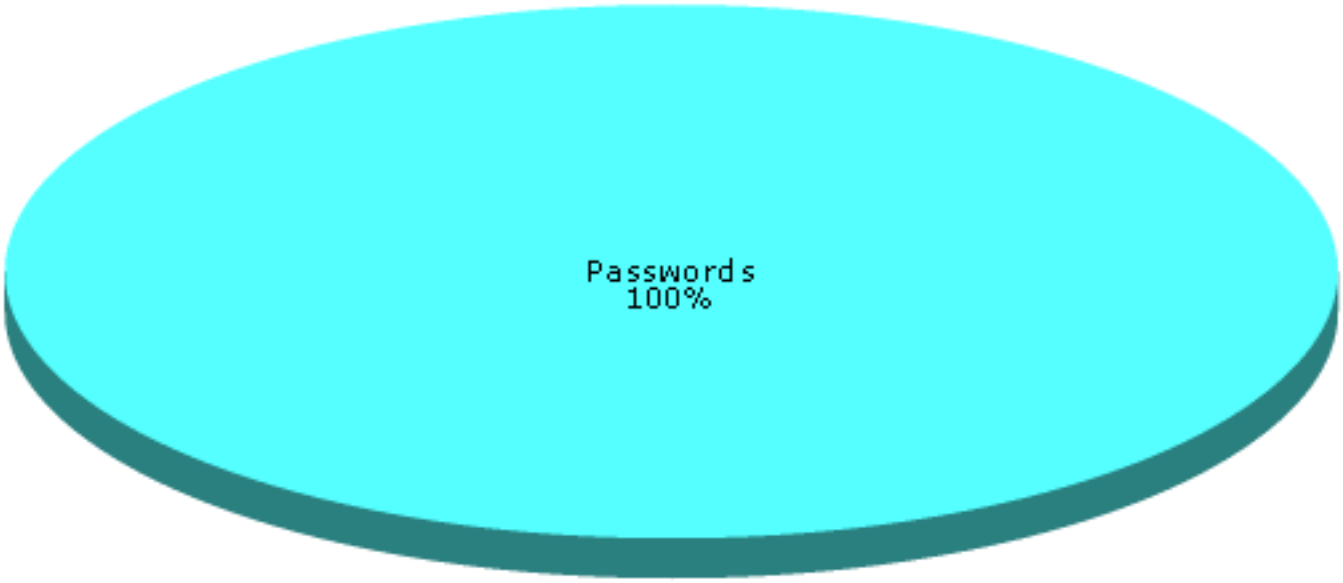




2.3 Exploited Vulnerabilities by Class

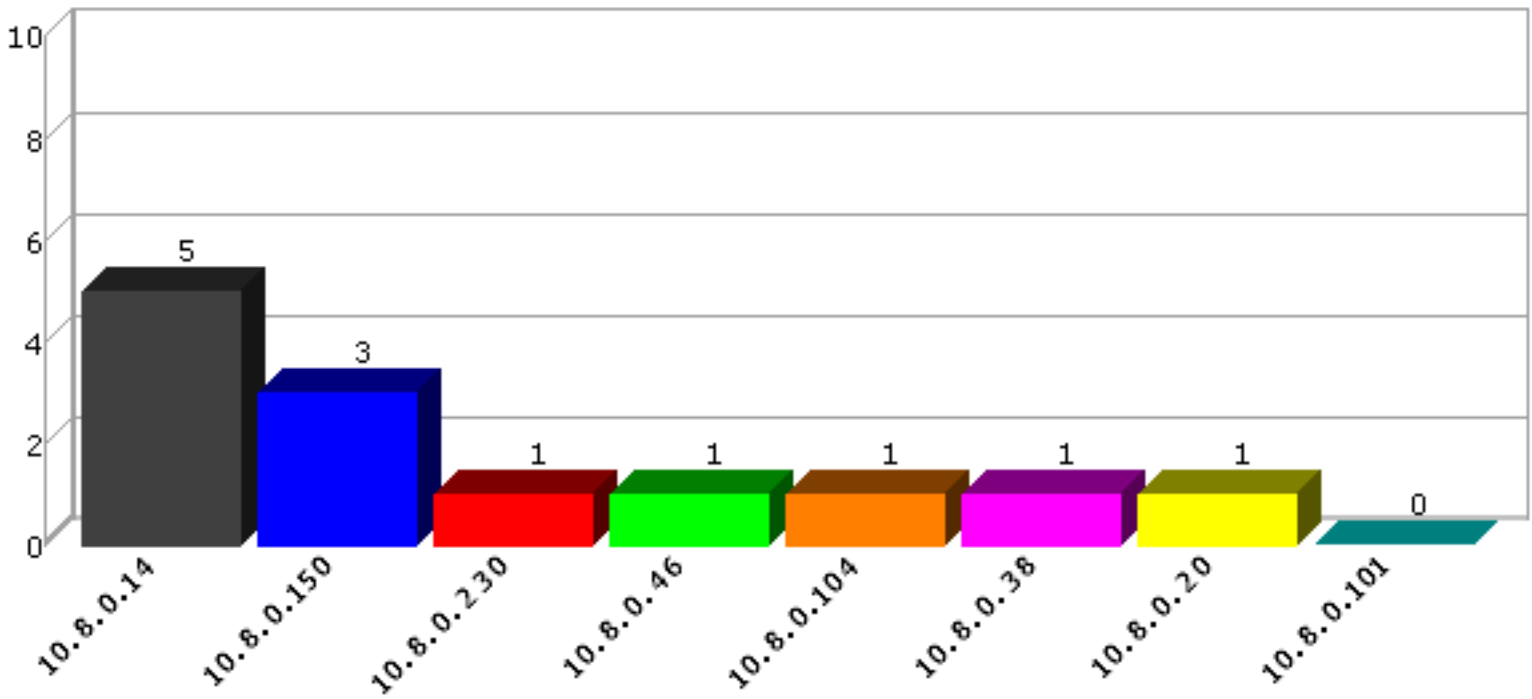
This section shows the number of vulnerabilities exploited in each vulnerability class.





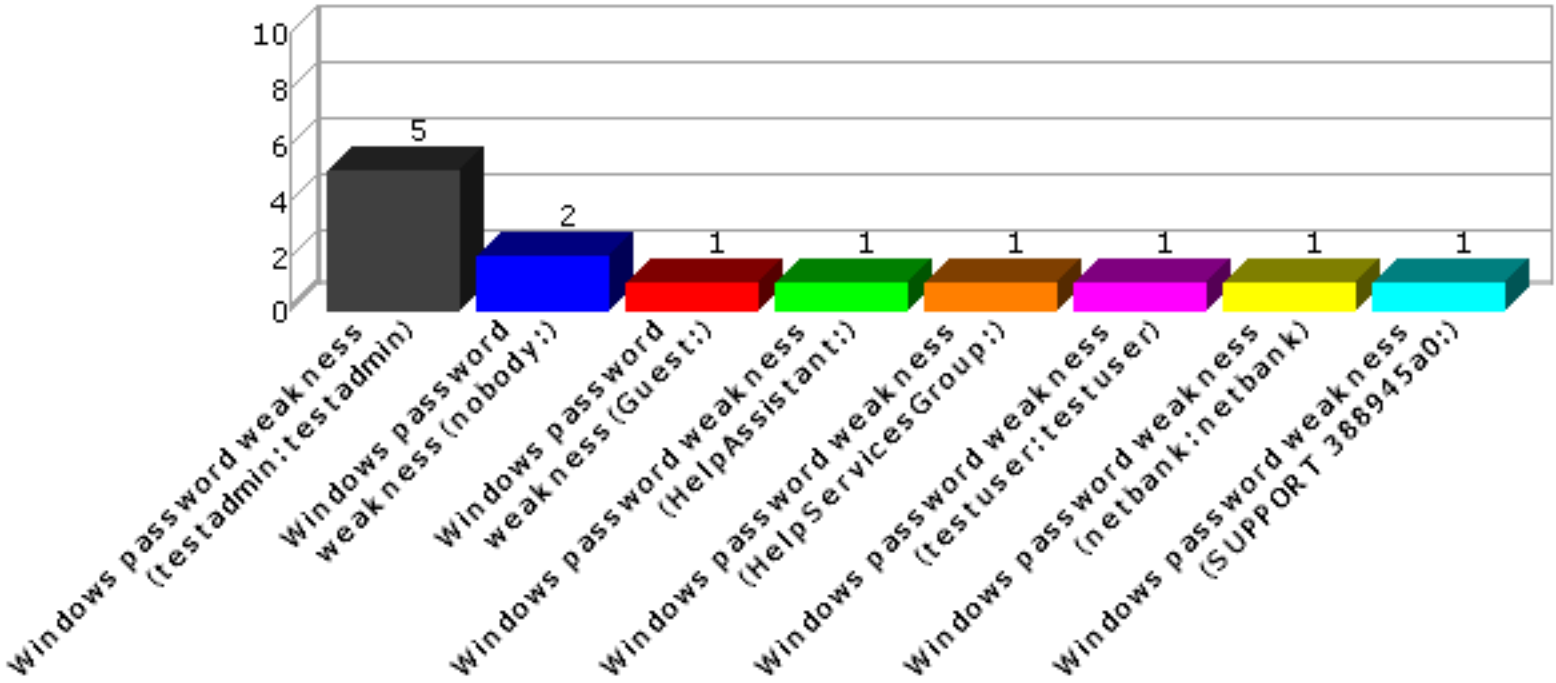
2.4 Top 10 Vulnerable Hosts

This section shows the most vulnerable hosts detected, and the number of successful exploits run against them.



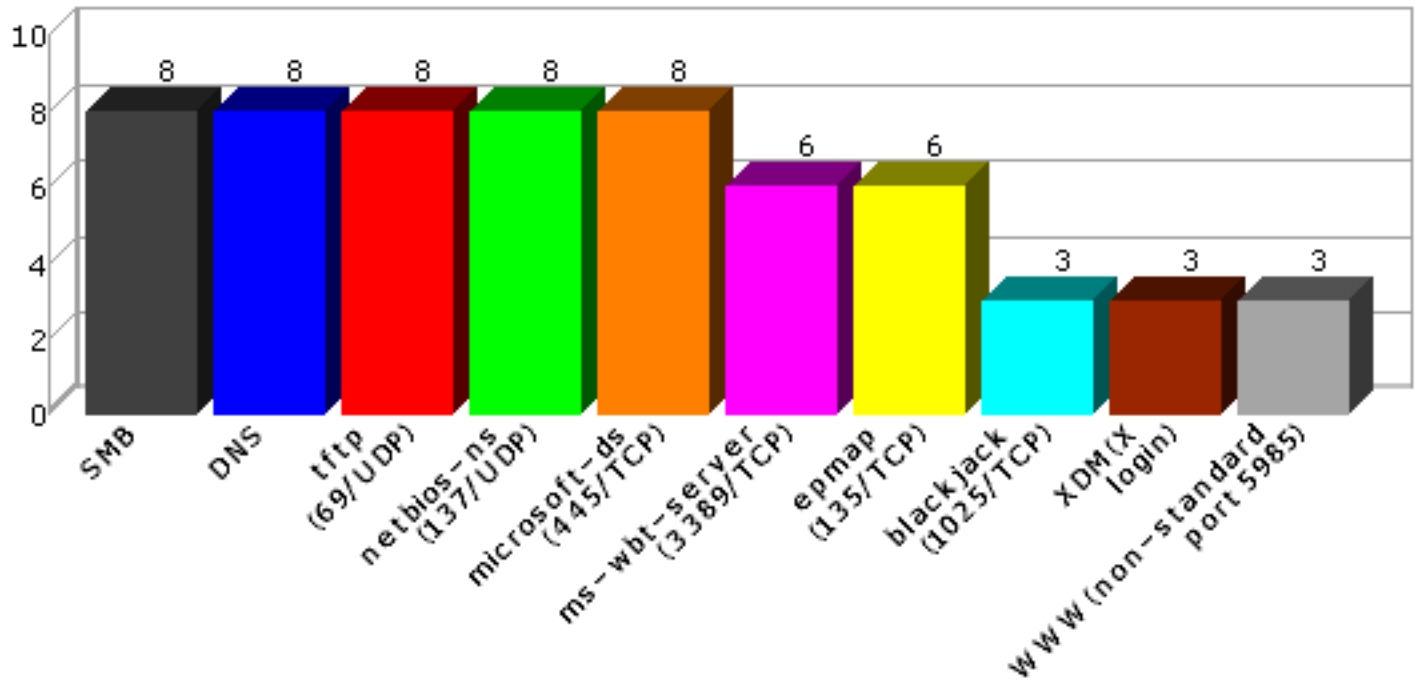
2.5 Top 10 Successful Exploits

This section shows the most successful exploits, and the number of occurrences.



2.6 Top 10 Services

This section shows the most common services detected, and the number of hosts on which they were detected.



3 Overview

The following tables present an overview of the hosts discovered on the network and the access level gained on each.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Remote Admin	Privilege Elevation	Remote User	Client Access	Unsuccessful Exploits
10.8.0.14	XPPROUNPATCHED	10.8.0.14	Windows XP SP2	0	0	5	0	101
10.8.0.20	WIN81	10.8.0.20	Windows 8.1	0	0	1	0	76
10.8.0.38	WIN7	10.8.0.38	Windows 7 SP1	0	0	1	0	161
10.8.0.46	SAINT84VM64	10.8.0.46	Ubuntu 14.04	1	0	0	0	16
10.8.0.101	WIN2003PATCHED	10.8.0.101	Windows Server 2003 SP2	0	0	0	0	194
10.8.0.104	XPSP3PATCHED	10.8.0.104	Windows XP SP3	0	0	1	0	172
10.8.0.150	WIN-IQF3U12CJA5	10.8.0.150	Windows Server 2008 R2	0	0	3	0	322
10.8.0.230	UBUNTUNESSUS	10.8.0.230	Linux 3.13.0-57-generic - Ubuntu 14.04	1	0	0	0	35

3.2 Exploit Summary List

This table lists the number of times each exploit succeeded on the network.

Exploit	Occurrences
Windows password weakness (testadmin:testadmin)	5
Windows password weakness (nobody:)	2
Windows password weakness (Guest:)	1
Windows password weakness (HelpAssistant:)	1
Windows password weakness (HelpServicesGroup:)	1
Windows password weakness (testuser:testuser)	1
Windows password weakness (netbank:netbank)	1
Windows password weakness (SUPPORT_388945a0:)	1

3.3 Exploit List

This table presents an overview of the exploits executed on the network.

Host Name	Port	Result	Vulnerability / Service	Class	CVE
10.8.0.14	139 /tcp	remote user	Windows password weakness (Guest:)	Passwords	CVE-1999-0503
10.8.0.14	139 /tcp	remote user	Windows password weakness (HelpAssistant:)	Passwords	CVE-1999-0503
10.8.0.14	139 /tcp	remote user	Windows password weakness (HelpServicesGroup:)	Passwords	CVE-1999-0503
10.8.0.14	139 /tcp	remote user	Windows password weakness (SUPPORT_388945a0:)	Passwords	CVE-1999-0503
10.8.0.14	139 /tcp	remote user	Windows password weakness (testadmin:testadmin)	Passwords	CVE-1999-0503
10.8.0.14	69/udp	unsuccessful exploit	3Com TFTP server Transporting Mode buffer overflow	File Transfer	CVE-2006-6183
10.8.0.14	80/tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.14	80/tcp	unsuccessful exploit	Apache mod_rewrite LDAP URL buffer overflow	Web	CVE-2006-3747
10.8.0.14	80/tcp	unsuccessful exploit	AWStats configdir parameter command execution	Web	CVE-2005-0116
10.8.0.14	80/tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.14	80/tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.14	80/tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.14	80/tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.14	80/tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.14	80/tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.14	80/tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.14	80/tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.14	80/tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.14	80/tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.14	80/tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.14	80/tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.14	80/tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.14	80/tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.14	80/tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.14	80/tcp	unsuccessful exploit	GitList blame resource command injection	Web	CVE-2014-4511

10.8.0.14	80/tcp	unsuccessful exploit	Hastymail rs parameter command injection	Web	CVE-2011-4542
10.8.0.14	80/tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.14	80/tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.14	80/tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.14	80/tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.14	80/tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.14	80/tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.14	80/tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.14	80/tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.14	80/tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.14	80/tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.14	80/tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.14	80/tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.14	80/tcp	unsuccessful exploit	IIS Double Decoding Directory Traversal	Web	CVE-2001-0333
10.8.0.14	80/tcp	unsuccessful exploit	IIS Unicode Directory Traversal	Web	CVE-2000-0884
10.8.0.14	80/tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.14	80/tcp	unsuccessful exploit	JRun mod_jrun WriteToLog buffer overflow	Web	CVE-2004-0646
10.8.0.14	80/tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.14	80/tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.14	80/tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.14	80/tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.14	80/tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.14	80/tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.14	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
10.8.0.14	445 /tcp	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
10.8.0.14	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
10.8.0.14	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.14	80/tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929

10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.14	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.14	80/tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.14	80/tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.14	80/tcp	unsuccessful exploit	PHP Remote File Inclusion	Web	
10.8.0.14	80/tcp	unsuccessful exploit	phpBB viewtopic.php highlight parameter vulnerability	Web	CVE-2005-2086
10.8.0.14	80/tcp	unsuccessful exploit	phpRPC decode function command execution	Web	CVE-2006-1032
10.8.0.14	80/tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.14	80/tcp	unsuccessful exploit	RSA Authentication Agent for Web for IIS chunked encoding overflow	Web	CVE-2005-1471
10.8.0.14	80/tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.14	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.14	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.14	80/tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.14	3133 /udp	unsuccessful exploit	Snort Back Orifice Pre-Processor buffer overflow	Other	CVE-2005-3252
10.8.0.14	445 /tcp	unsuccessful exploit	Snort DCE/RPC preprocessor buffer overflow	Other	CVE-2006-5276
10.8.0.14	80/tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.14	80/tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.14	80/tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.14	80/tcp	unsuccessful exploit	Sun Java System Web Server WebDAV OPTIONS request buffer overflow	Web	CVE-2010-0361

10.8.0.14	80/tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.14	80/tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.14	80/tcp	unsuccessful exploit	Traq authenticate function remote code execution	Web	
10.8.0.14	80/tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.14	80/tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.14	80/tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.14	80/tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.14	80/tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.14	80/tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.14	80/tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.14	80/tcp	unsuccessful exploit	Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow	Web	CVE-2008-4008
10.8.0.14	80/tcp	unsuccessful exploit	WhatsUp Gold _maincfgret.cgi instancename buffer overflow	Web	CVE-2004-0798
10.8.0.14	445 /tcp	unsuccessful exploit	Windows LSASS buffer overflow	Windows OS	CVE-2003-0533
10.8.0.14	445 /tcp	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
10.8.0.14	445 /tcp	unsuccessful exploit	Windows Server Service buffer overflow	Windows OS	CVE-2006-3439
10.8.0.14	445 /tcp	unsuccessful exploit	Windows Server Service buffer overflow MS08-067	Windows OS	CVE-2008-4250
10.8.0.14	445 /tcp	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
10.8.0.14		unsuccessful exploit	Wireshark DECT Dissector Remote Stack Buffer Overflow	Other	CVE-2011-1591
10.8.0.14	80/tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.14	80/tcp	unsuccessful exploit	Xi Software Net Transport eDonkey Protocol Buffer Overflow	Other	
10.8.0.14	80/tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.14	80/tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.14	80/tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.14	1026 /udp	service	1026/UDP		
10.8.0.14	53/udp	service	DNS		
10.8.0.14	139 /tcp	service	SMB		
10.8.0.14	80/tcp	service	WWW		
10.8.0.14	177 /udp	service	XDM (X login)		
10.8.0.14	1025 /udp	service	blackjack (1025/UDP)		
10.8.0.14	135 /tcp	service	epmap (135/TCP)		

10.8.0.14	1718 /udp	service	h323gatedisc (1718/UDP)		
10.8.0.14	1719 /udp	service	h323gatestat (1719/UDP)		
10.8.0.14	500 /udp	service	isakmp (500/UDP)		
10.8.0.14	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.14	445 /udp	service	microsoft-ds (445/UDP)		
10.8.0.14	3389 /tcp	service	ms-wbt-server (3389/TCP)		
10.8.0.14	138 /udp	service	netbios-dgm (138/UDP)		
10.8.0.14	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.14	123 /udp	service	ntp (123/UDP)		
10.8.0.14	1900 /udp	service	ssdp (1900/UDP)		
10.8.0.14	69/udp	service	tftp (69/UDP)		
10.8.0.20	139 /tcp	remote user	Windows password weakness (testadmin:testadmin)	Passwords	CVE-1999-0503
10.8.0.20	5357 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.20	5357 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.20	5357 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.20	5357 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.20	5357 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.20	5357 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.20	5357 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.20	5357 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.20	5357 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.20	5357 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.20	5357 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.20	5357 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.20	5357 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822

10.8.0.20	5357 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.20	5357 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.20	5357 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.20	5357 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.20	5357 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.20	5357 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.20	5357 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.20	5357 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.20	5357 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.20	5357 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.20	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
10.8.0.20	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.20	5357 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.20	5357 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067

10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.20	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.20	5357 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.20	5357 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.20	5357 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.20	5357 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.20	5357 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.20	5357 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.20	5357 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.20	5357 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.20	5357 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.20	5357 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.20	5357 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.20	69/udp	unsuccessful exploit	TFTP Server error packet buffer overflow	File Transfer	CVE-2008-2161
10.8.0.20	5357 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.20	5357 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.20	5357 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.20	5357 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.20	5357 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.20	5357 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.20	5357 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.20	5357 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.20	445 /tcp	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
10.8.0.20	445 /tcp	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
10.8.0.20		unsuccessful exploit	Wireshark DECT Dissector Remote Stack Buffer Overflow	Other	CVE-2011-1591
10.8.0.20	5357 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.20	5357 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.20	5357 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	

10.8.0.20	5357 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.20	5357 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.20	2179 /tcp	service	2179/TCP		
10.8.0.20	53/udp	service	DNS		
10.8.0.20	139 /tcp	service	SMB		
10.8.0.20	5357 /tcp	service	WWW (non-standard port 5357)		
10.8.0.20	135 /tcp	service	epmap (135/TCP)		
10.8.0.20	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.20	3389 /tcp	service	ms-wbt-server (3389/TCP)		
10.8.0.20	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.20	69/udp	service	tftp (69/UDP)		
10.8.0.38	139 /tcp	remote user	Windows password weakness (testadmin:testadmin)	Passwords	CVE-1999-0503
10.8.0.38	5357 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.38	5357 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.38	5985 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.38	5357 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.38	5357 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.38	5985 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.38	5985 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.38	5357 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.38	5357 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.38	5985 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.38	5357 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.38	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.38	5357 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.38	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.38	5357 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733

10.8.0.38	5985 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.38	5985 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.38	5357 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.38	21/tcp	unsuccessful exploit	Easy FTP Server MKD command buffer overflow	File Transfer	
10.8.0.38	5357 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.38	5357 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.38	5985 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.38	5357 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.38	21/tcp	unsuccessful exploit	Freefloat FTP Server USER Command Buffer Overflow	File Transfer	
10.8.0.38	21/tcp	unsuccessful exploit	Freefloat FTPD Invalid Command Overflow	File Transfer	
10.8.0.38	5985 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.38	5357 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.38	5357 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.38	5985 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999

10.8.0.38	5985 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.38	5985 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.38	5357 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.38	5985 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.38	5357 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.38	5357 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.38	5985 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.38	5357 /tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.38	5985 /tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.38	5357 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.38	5357 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.38	5985 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.38	5985 /tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.38	5357 /tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.38	5357 /tcp	unsuccessful exploit	Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow	Web	CVE-2014-5289
10.8.0.38	21/tcp	unsuccessful exploit	Konica Minolta FTP Utility buffer overflow	File Transfer	
10.8.0.38	5985 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.38	5985 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.38	5985 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.38	5985 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.38	5357 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.38	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206

10.8.0.38	445 /tcp	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
10.8.0.38	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
10.8.0.38	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.38	5985 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.38	5357 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.38	21/tcp	unsuccessful exploit	Open and Compact FTP Server Long Password Buffer Overflow	File Transfer	
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181

10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.38	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.38	5357 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.38	5985 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.38	5985 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.38	5985 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.38	5357 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.38	5985 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.38	21/tcp	unsuccessful exploit	Ricoh DC Software DL-10 FTP Server USER Remote Code Execution	File Transfer	
10.8.0.38	5357 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.38	5357 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.38	5985 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.38	5357 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.38	5985 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.38	5985 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.38	5985 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.38	5357 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.38	5985 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.38	69/udp	unsuccessful exploit	TFTP Server error packet buffer overflow	File Transfer	CVE-2008-2161
10.8.0.38	5985 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.38	5357 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602

10.8.0.38	5357 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.38	5985 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.38	5357 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.38	5985 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.38	5357 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.38	5985 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.38	5357 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.38	5985 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.38	5985 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.38	5357 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.38	5357 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.38	5985 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.38	5985 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.38	5357 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.38	445 /tcp	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
10.8.0.38	445 /tcp	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
10.8.0.38		unsuccessful exploit	Wireshark DECT Dissector Remote Stack Buffer Overflow	Other	CVE-2011-1591
10.8.0.38	5357 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.38	5985 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.38	21/tcp	unsuccessful exploit	WS_FTP MKD command buffer overflow	File Transfer	CVE-2004-1135
10.8.0.38	5985 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.38	5357 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.38	5357 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.38	5357 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.38	5985 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.38	5357 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.38	5985 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.38	1026 /tcp	service	1026/TCP		

10.8.0.38	1027 /tcp	service	1027/TCP		
10.8.0.38	1033 /tcp	service	1033/TCP		
10.8.0.38	53/udp	service	DNS		
10.8.0.38	21/tcp	service	FTP		
10.8.0.38	139 /tcp	service	SMB		
10.8.0.38	5357 /tcp	service	WWW (non-standard port 5357)		
10.8.0.38	5985 /tcp	service	WWW (non-standard port 5985)		
10.8.0.38	1025 /tcp	service	blackjack (1025/TCP)		
10.8.0.38	135 /tcp	service	epmap (135/TCP)		
10.8.0.38	990 /tcp	service	ftps (990/TCP)		
10.8.0.38	1032 /tcp	service	iad3 (1032/TCP)		
10.8.0.38	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.38	3389 /tcp	service	ms-wbt-server (3389/TCP)		
10.8.0.38	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.38	1057 /tcp	service	startron (1057/TCP)		
10.8.0.38	69/udp	service	tftp (69/UDP)		
10.8.0.46	139 /tcp	remote admin	Windows password weakness (nobody:)	Passwords	CVE-1999-0503
10.8.0.46	443 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.46	443 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.46	443 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.46	443 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.46	443 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.46	443 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.46	443 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.46	443 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.46	443 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.46	22/tcp	unsuccessful exploit	F5 BIG-IP SSH private key	Other	CVE-2012-1493
10.8.0.46	22/tcp	unsuccessful exploit	Symantec Messaging Gateway Default SSH Password	Passwords	CVE-2012-3579
10.8.0.46	443 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.46	443 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877

10.8.0.46	443 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.46	443 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.46	443 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.46	623 /tcp	service	623/TCP		
10.8.0.46	53/udp	service	DNS		
10.8.0.46	139 /tcp	service	SMB		
10.8.0.46	22/tcp	service	SSH		
10.8.0.46	443 /tcp	service	WWW (Secure)		
10.8.0.46	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.46	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.46	111 /tcp	service	sunrpc (111/TCP)		
10.8.0.46	69/udp	service	tftp (69/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-2 portmapper (111/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-2 portmapper (111/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-3 portmapper (111/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-3 portmapper (111/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-4 portmapper (111/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100000-4 portmapper (111/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100007-1 ypbind (622/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100007-1 ypbind (623/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100007-2 ypbind (622/UDP)		
10.8.0.46	111 /tcp	info	RPC service: 100007-2 ypbind (623/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100024-1 status (40667/TCP)		
10.8.0.46	111 /tcp	info	RPC service: 100024-1 status (57303/UDP)		
10.8.0.101	8080 /tcp	unsuccessful exploit	Smart Software Solutions CoDeSys Webserver URI Copying Stack Buffer Overflow	Web	CVE-2011-5007
10.8.0.101	8000 /tcp	unsuccessful exploit	Smart Software Solutions CoDeSys Webserver URI Copying Stack Buffer Overflow	Web	CVE-2011-5007
10.8.0.101	8080 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.101	8080 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.101	8000 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811

10.8.0.101	8080 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.101	8000 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.101	8000 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.101	8080 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.101	8080 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.101	8000 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.101	8080 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.101	8000 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.101	445 /tcp	unsuccessful exploit	Computer Associates Alert Notification Server buffer overflow	Other	CVE-2007-3825
10.8.0.101	445 /tcp	unsuccessful exploit	Computer Associates Alert Notification Server opcode 23 buffer overflow	Other	CVE-2007-4620
10.8.0.101	8080 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.101	8000 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.101	8080 /tcp	unsuccessful exploit	Cisco Secure ACS UCP CSuserCGI.exe buffer overflow	Web	CVE-2008-0532
10.8.0.101	8000 /tcp	unsuccessful exploit	Cisco Secure ACS UCP CSuserCGI.exe buffer overflow	Web	CVE-2008-0532
10.8.0.101	8080 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.101	8000 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.101	8000 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.101	8080 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.101	8000 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.101	8080 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.101	8000 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.101	8080 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.101	8080 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.101	8080 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.101	8000 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928

10.8.0.101	8080 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.101	8000 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.101	8000 /tcp	unsuccessful exploit	Free Download Manager Remote Control Server HTTP Authorization buffer overflow	Web	CVE-2009-0183
10.8.0.101	8080 /tcp	unsuccessful exploit	Free Download Manager Remote Control Server HTTP Authorization buffer overflow	Web	CVE-2009-0183
10.8.0.101	8080 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.101	8000 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.101	8080 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.101	8000 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.101	8080 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.101	8080 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.101	8000 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.101	8000 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.101	8080 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.101	8000 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219

10.8.0.101	8000 /tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.101	8080 /tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.101	8080 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.101	8080 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.101	8000 /tcp	unsuccessful exploit	JRun mod_jrun WriteToLog buffer overflow	Web	CVE-2004-0646
10.8.0.101	8080 /tcp	unsuccessful exploit	JRun mod_jrun WriteToLog buffer overflow	Web	CVE-2004-0646
10.8.0.101	8000 /tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.101	8080 /tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.101	8000 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.101	8080 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.101	8000 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.101	8080 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.101	8000 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.101	8000 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.101	8080 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.101	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
10.8.0.101	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
10.8.0.101	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll EnumPrinters buffer overflow	Other	CVE-2008-0639
10.8.0.101	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.101	8080 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554

10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OvOSLocale cookie buffer overflow	Web	CVE-2009-0920
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OvOSLocale cookie buffer overflow	Web	CVE-2009-0920
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil.dll stringToSeconds Buffer Overflow	Web	CVE-2011-0262
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil.dll stringToSeconds Buffer Overflow	Web	CVE-2011-0262
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.101	8080 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.101	8000 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle Database Advanced Replication component DBMS_SNAP_INTERNAL overflow	Other	CVE-2007-2116

10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle Database Advanced Replication component DBMS_SNAP_INTERNAL overflow	Other	CVE-2007-2116
10.8.0.101	8000 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.101	8000 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.101	1521	unsuccessful exploit	Oracle password weakness	Other	
10.8.0.101	1051	unsuccessful exploit	Oracle password weakness	Other	
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle MD2 component SDO_CODE_SIZE buffer overflow	Other	CVE-2004-1774
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle MD2 component SDO_CODE_SIZE buffer overflow	Other	CVE-2004-1774
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle Database OLAP component ODCITABLESTART buffer overflow	Other	CVE-2008-3974
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle Database OLAP component ODCITABLESTART buffer overflow	Other	CVE-2008-3974
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle Spatial component SDO_CS.TRANSFORM_LAYER buffer overflow	Other	CVE-2006-5344
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle Spatial component SDO_CS.TRANSFORM_LAYER buffer overflow	Other	CVE-2006-5344
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle Database string conversion buffer overflow	Other	
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle Database string conversion buffer overflow	Other	
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle Warehouse Builder SQL Injection	Other	CVE-2011-0799
10.8.0.101	8080 /tcp	unsuccessful exploit	Oracle 9i Release 2 XDB HTTP Pass Overflow	Web	CVE-2003-0727
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle XDB component PITRIG_DROPMETADATA buffer overflow	Other	CVE-2007-4517
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle XDB component PITRIG_DROPMETADATA buffer overflow	Other	CVE-2007-4517
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle XDB component PITRIG_TRUNCATE buffer overflow	Other	CVE-2008-0339
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle XDB component PITRIG_TRUNCATE buffer overflow	Other	CVE-2008-0339
10.8.0.101	1051 /tcp	unsuccessful exploit	Oracle XML Component DBMS_XMLSCHEMA.GENERATESCHEMA buffer overflow	Other	CVE-2006-0272
10.8.0.101	1521 /tcp	unsuccessful exploit	Oracle XML Component DBMS_XMLSCHEMA.GENERATESCHEMA buffer overflow	Other	CVE-2006-0272
10.8.0.101	8000 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.101	8080 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.101	8080 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.101	8080 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.101	8000 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	

10.8.0.101	8000 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.101	8000 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.101	8000 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.101	8080 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.101	139 /tcp	unsuccessful exploit	Windows password weakness	Passwords	CVE-1999-0503
10.8.0.101	8000 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.101	8080 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.101	8080 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.101	8000 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.101	8000 /tcp	unsuccessful exploit	SQL injection authentication bypass	Web	
10.8.0.101	8000 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.101	8000 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.101	8080 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.101	8000 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.101	69/udp	unsuccessful exploit	TFTP Server error packet buffer overflow	File Transfer	CVE-2008-2161
10.8.0.101	8080 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.101	8000 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.101	8000 /tcp	unsuccessful exploit	Trend Micro OfficeScan CGI programs POST request buffer overflow	Web	CVE-2008-3862
10.8.0.101	8080 /tcp	unsuccessful exploit	Trend Micro OfficeScan CGI programs POST request buffer overflow	Web	CVE-2008-3862
10.8.0.101	8000 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.101	8080 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.101	8080 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.101	8000 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.101	8000 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.101	8080 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.101	8080 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.101	8000 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.101	8000 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236

10.8.0.101	8080 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.101	8080 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.101	8000 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.101	8000 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.101	135 /tcp	unsuccessful exploit	Windows DNS server RPC management interface buffer overflow	RPC	CVE-2007-1748
10.8.0.101	135 /tcp	unsuccessful exploit	Windows RPC DCOM interface buffer overflow	Windows OS	CVE-2003-0352
10.8.0.101	445 /tcp	unsuccessful exploit	Windows Server Service buffer overflow MS08-067	Windows OS	CVE-2008-4250
10.8.0.101	445 /tcp	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
10.8.0.101	8080 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.101	8000 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.101	8080 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.101	8080 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.101	8000 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.101	53/udp	service	DNS		
10.8.0.101	139 /tcp	service	SMB		
10.8.0.101	8000 /tcp	service	WWW (non-standard port 8000)		
10.8.0.101	8080 /tcp	service	WWW (non-standard port 8080)		
10.8.0.101	177 /udp	service	XDM (X login)		
10.8.0.101	1025 /tcp	service	blackjack (1025/TCP)		
10.8.0.101	135 /tcp	service	epmap (135/TCP)		
10.8.0.101	1718 /udp	service	h323gatedisc (1718/UDP)		
10.8.0.101	1719 /udp	service	h323gatestat (1719/UDP)		
10.8.0.101	500 /udp	service	isakmp (500/UDP)		
10.8.0.101	1064 /udp	service	jstel (1064/UDP)		
10.8.0.101	1701 /udp	service	l2f (1701/UDP)		

10.8.0.101	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.101	445 /udp	service	microsoft-ds (445/UDP)		
10.8.0.101	3389 /tcp	service	ms-wbt-server (3389/TCP)		
10.8.0.101	1521 /tcp	service	ncube-lm (1521/TCP)		
10.8.0.101	138 /udp	service	netbios-dgm (138/UDP)		
10.8.0.101	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.101	123 /udp	service	ntp (123/UDP)		
10.8.0.101	1051 /tcp	service	optima-vnet (1051/TCP)		
10.8.0.101	1723 /tcp	service	pptp (1723/TCP)		
10.8.0.101	69/udp	service	tftp (69/UDP)		
10.8.0.104	139 /tcp	remote user	Windows password weakness (testadmin:testadmin)	Passwords	CVE-1999-0503
10.8.0.104	5985 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.104	80/tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Apache mod_rewrite LDAP URL buffer overflow	Web	CVE-2006-3747
10.8.0.104	80/tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.104	5985 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.104	80/tcp	unsuccessful exploit	AWStats configdir parameter command execution	Web	CVE-2005-0116
10.8.0.104	5985 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.104	80/tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.104	80/tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.104	5985 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.104	5985 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.104	80/tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.104	5985 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.104	80/tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.104	80/tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.104	80/tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.104	5985 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223

10.8.0.104	80/tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.104	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.104	80/tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.104	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.104	80/tcp	unsuccessful exploit	CMailServer CMailCOM.dll MoveToFolder buffer overflow	Mail	
10.8.0.104	80/tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.104	5985 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.104	5985 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.104	80/tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.104	5985 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.104	80/tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.104	5985 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.104	80/tcp	unsuccessful exploit	GitList blame resource command injection	Web	CVE-2014-4511
10.8.0.104	80/tcp	unsuccessful exploit	Hastymail rs parameter command injection	Web	CVE-2011-4542
10.8.0.104	80/tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.104	80/tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.104	5985 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.104	80/tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548

10.8.0.104	80/tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.104	80/tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.104	5985 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.104	80/tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.104	80/tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.104	5985 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.104	5985 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.104	80/tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.104	80/tcp	unsuccessful exploit	IIS Double Decoding Directory Traversal	Web	CVE-2001-0333
10.8.0.104	80/tcp	unsuccessful exploit	IIS Unicode Directory Traversal	Web	CVE-2000-0884
10.8.0.104	80/tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.104	80/tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.104	80/tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.104	5985 /tcp	unsuccessful exploit	Kolibri WebServer HTTP GET Request Handling Buffer Overflow	Web	CVE-2014-4158
10.8.0.104	5985 /tcp	unsuccessful exploit	Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow	Web	CVE-2014-5289
10.8.0.104	80/tcp	unsuccessful exploit	Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow	Web	CVE-2014-5289
10.8.0.104	80/tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.104	5985 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.104	80/tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.104	80/tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.104	3306 /tcp	unsuccessful exploit	MySQL password weakness	Other	

10.8.0.104	80/tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.104	5985 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.104	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
10.8.0.104	445 /tcp	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
10.8.0.104	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
10.8.0.104	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.104	80/tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204

10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.104	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.104	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.104	80/tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.104	80/tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.104	5985 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.104	80/tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.104	80/tcp	unsuccessful exploit	PHP Remote File Inclusion	Web	
10.8.0.104	80/tcp	unsuccessful exploit	phpBB viewtopic.php highlight parameter vulnerability	Web	CVE-2005-2086
10.8.0.104	80/tcp	unsuccessful exploit	phpRPC decode function command execution	Web	CVE-2006-1032
10.8.0.104	5985 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.104	80/tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.104	80/tcp	unsuccessful exploit	RSA Authentication Agent for Web for IIS chunked encoding overflow	Web	CVE-2005-1471
10.8.0.104	5985 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.104	80/tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.104	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.104	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.104	80/tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.104	80/tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.104	5985 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.104	80/tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251

10.8.0.104	80/tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.104	5985 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.104	5985 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.104	80/tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.104	69/udp	unsuccessful exploit	TFTP Server error packet buffer overflow	File Transfer	CVE-2008-2161
10.8.0.104	80/tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.104	5985 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.104	80/tcp	unsuccessful exploit	Traq authenticate function remote code execution	Web	
10.8.0.104	80/tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.104	5985 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.104	80/tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.104	80/tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.104	5985 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.104	5985 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.104	80/tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.104	80/tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.104	5985 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.104	80/tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.104	5985 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.104	80/tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.104	80/tcp	unsuccessful exploit	Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow	Web	CVE-2008-4008
10.8.0.104	80/tcp	unsuccessful exploit	WhatsUp Gold _maincfgret.cgi instancename buffer overflow	Web	CVE-2004-0798
10.8.0.104	445 /tcp	unsuccessful exploit	Windows LSASS buffer overflow	Windows OS	CVE-2003-0533
10.8.0.104	445 /tcp	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
10.8.0.104	135 /tcp	unsuccessful exploit	Windows RPC DCOM interface buffer overflow	Windows OS	CVE-2003-0352
10.8.0.104	445 /tcp	unsuccessful exploit	Windows RRAS memory corruption vulnerability	Windows OS	CVE-2006-2370
10.8.0.104	445 /tcp	unsuccessful exploit	Windows Server Service buffer overflow MS08-067	Windows OS	CVE-2008-4250
10.8.0.104		unsuccessful exploit	Wireshark DECT Dissector Remote Stack Buffer Overflow	Other	CVE-2011-1591
10.8.0.104	80/tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021

10.8.0.104	5985 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.104	80/tcp	unsuccessful exploit	Xi Software Net Transport eDonkey Protocol Buffer Overflow	Other	
10.8.0.104	80/tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.104	80/tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.104	80/tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.104	80/tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.104	5985 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.104	53/udp	service	DNS		
10.8.0.104	139 /tcp	service	SMB		
10.8.0.104	80/tcp	service	WWW		
10.8.0.104	5985 /tcp	service	WWW (non-standard port 5985)		
10.8.0.104	177 /udp	service	XDM (X login)		
10.8.0.104	135 /tcp	service	epmap (135/TCP)		
10.8.0.104	1718 /udp	service	h323gatedisc (1718/UDP)		
10.8.0.104	1719 /udp	service	h323gatestat (1719/UDP)		
10.8.0.104	500 /udp	service	isakmp (500/UDP)		
10.8.0.104	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.104	445 /udp	service	microsoft-ds (445/UDP)		
10.8.0.104	3389 /tcp	service	ms-wbt-server (3389/TCP)		
10.8.0.104	3306 /tcp	service	mysql (3306/TCP)		
10.8.0.104	138 /udp	service	netbios-dgm (138/UDP)		
10.8.0.104	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.104	123 /udp	service	ntp (123/UDP)		
10.8.0.104	1900 /udp	service	ssdp (1900/UDP)		
10.8.0.104	69/udp	service	tftp (69/UDP)		
10.8.0.150	139 /tcp	remote user	Windows password weakness (netbank:netbank)	Passwords	CVE-1999-0503
10.8.0.150	139 /tcp	remote user	Windows password weakness (testadmin:testadmin)	Passwords	CVE-1999-0503

10.8.0.150	139 /tcp	remote user	Windows password weakness (testuser:testuser)	Passwords	CVE-1999-0503
10.8.0.150	8059 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.150	80/tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Apache mod_rewrite LDAP URL buffer overflow	Web	CVE-2006-3747
10.8.0.150	8059 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.150	80/tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.150	5985 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.150	8082 /tcp	unsuccessful exploit	Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload	Web	CVE-2012-3811
10.8.0.150	80/tcp	unsuccessful exploit	AWStats configdir parameter command execution	Web	CVE-2005-0116
10.8.0.150	8059 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.150	5985 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.150	80/tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.150	8082 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.150	5985 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.150	8082 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.150	8059 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.150	80/tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.150	8059 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.150	80/tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.150	8082 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.150	5985 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.150	80/tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.150	8059 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.150	5985 /tcp	unsuccessful exploit	CA ARCserve D2D Axis2 default password	Web	CVE-2010-0219
10.8.0.150	8059 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.150	8082 /tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	

10.8.0.150	80/tcp	unsuccessful exploit	CA Total Defense UNCWS exportReport SQL Injection	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.150	8082 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.150	8059 /tcp	unsuccessful exploit	CA XOsoft Control Service entry_point.aspx Remote Code Execution	Web	CVE-2010-1223
10.8.0.150	8059 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.150	8082 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.150	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.150	80/tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.150	5985 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.150	8082 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.150	80/tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.150	8059 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.150	80/tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.150	8059 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.150	8082 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.150	5985 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.150	80/tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	Easy Chat Server Authentication Request Buffer Overflow	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	Easy File Management Web Server UserID Cookie Handling Buffer Overflow	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.150	5985 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791

10.8.0.150	8059 /tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.150	80/tcp	unsuccessful exploit	Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow	Web	CVE-2014-3791
10.8.0.150	5985 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.150	8082 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.150	8059 /tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.150	80/tcp	unsuccessful exploit	EMC AlphaStor Device Manager Command Injection	Other	CVE-2013-0928
10.8.0.150	80/tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.150	8082 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication Bypass	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.150	80/tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.150	5985 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.150	8082 /tcp	unsuccessful exploit	FrontPage fp30reg.dll remote debug buffer overflow	Web	CVE-2003-0822
10.8.0.150	80/tcp	unsuccessful exploit	GitList blame resource command injection	Web	CVE-2014-4511
10.8.0.150	80/tcp	unsuccessful exploit	Hastymail rs parameter command injection	Web	CVE-2011-4542
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.150	80/tcp	unsuccessful exploit	HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation	Web	CVE-2012-5201
10.8.0.150	8059 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.150	80/tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.150	8082 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.150	5985 /tcp	unsuccessful exploit	HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal	Web	CVE-2013-4837
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.150	80/tcp	unsuccessful exploit	HP Operations Agent Opcode 0x34 vulnerability	Web	CVE-2012-2019
10.8.0.150	80/tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020

10.8.0.150	5985 /tcp	unsuccessful exploit	HP Operations Agent Opcode 0x8c vulnerability	Web	CVE-2012-2020
10.8.0.150	80/tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Operations Manager hidden Tomcat account	Web	CVE-2009-3843
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Performance Insight Server Backdoor Account	Web	CVE-2011-0276
10.8.0.150	80/tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Performance Manager Apache Tomcat Policy Bypass	Web	CVE-2009-3548
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.150	80/tcp	unsuccessful exploit	HP Power Manager formExportDataLogs buffer overflow	Web	CVE-2009-3999
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.150	80/tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Power Manager formLogin buffer overflow	Web	CVE-2010-4113
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.150	8082 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.150	80/tcp	unsuccessful exploit	HP Power Manager Remote Code Execution	Web	CVE-2009-2685
10.8.0.150	80/tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.150	8082 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.150	8059 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.150	5985 /tcp	unsuccessful exploit	HP SiteScope SOAP Call APIPreferenceImpl Security Bypass	Other	CVE-2012-3261
10.8.0.150	5985 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.150	8059 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367

10.8.0.150	8082 /tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.150	80/tcp	unsuccessful exploit	HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability	Other	CVE-2013-2367
10.8.0.150	8059 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.150	5985 /tcp	unsuccessful exploit	HP Universal CMDB Server Axis2 default password	Web	CVE-2010-0219
10.8.0.150	8082 /tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.150	80/tcp	unsuccessful exploit	IBM Rational Quality Manager and Test Lab Manager Policy Bypass	Web	CVE-2010-4094
10.8.0.150	80/tcp	unsuccessful exploit	IIS Double Decoding Directory Traversal	Web	CVE-2001-0333
10.8.0.150	80/tcp	unsuccessful exploit	IIS Unicode Directory Traversal	Web	CVE-2000-0884
10.8.0.150	389 /tcp	unsuccessful exploit	IMail LDAP buffer overflow	Mail	CVE-2004-0297
10.8.0.150	5985 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	InterSystems Cache HTTP Stack Buffer Overflow	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.150	80/tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.150	5985 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.150	8059 /tcp	unsuccessful exploit	RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass	Web	CVE-2010-0738
10.8.0.150	8059 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.150	8082 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.150	5985 /tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.150	80/tcp	unsuccessful exploit	LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	Web	CVE-2012-1195
10.8.0.150	8059 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Lotus Domino HPRAgentName Stack Overflow	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.150	80/tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	McAfee Firewall Reporter isValidClient Authentication Bypass	Other	
10.8.0.150	80/tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.150	5985 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.150	8059 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810

10.8.0.150	8082 /tcp	unsuccessful exploit	McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	Other	CVE-2013-4810
10.8.0.150	8082 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.150	5985 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.150	80/tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.150	8059 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.150	139 /tcp	unsuccessful exploit	Windows NetDDE buffer overflow	Windows OS	CVE-2004-0206
10.8.0.150	445 /tcp	unsuccessful exploit	Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability	Other	CVE-2009-1350
10.8.0.150	445 /tcp	unsuccessful exploit	Novell Client nwspool.dll buffer overflow	Other	CVE-2006-5854
10.8.0.150	445 /tcp	unsuccessful exploit	Novell Client 4.91 SP4 nwspool.dll buffer overflow	Windows OS	CVE-2007-6701
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.150	80/tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell iManager EnteredClassName buffer overflow	Web	CVE-2010-1929
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Novell iManager getMultiPartParameters file upload vulnerability	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow	Web	CVE-2010-1555
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow	Web	CVE-2010-1554
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow	Web	CVE-2010-1553
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261

10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe	Web	CVE-2011-0261
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow	Web	CVE-2009-3848
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow	Web	CVE-2011-0268
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	Web	CVE-2011-0269
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OpenView5.exe buffer overflow	Web	CVE-2008-0067
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow	Web	CVE-2009-4179
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager OVBuildPath Overflow	Web	CVE-2011-3167
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovlogin.exe buffer overflow	Web	CVE-2007-6204
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe	Web	CVE-2009-4181
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552

10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow	Web	CVE-2010-1552
10.8.0.150	8082 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.150	5985 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.150	80/tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.150	8059 /tcp	unsuccessful exploit	HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow	Web	CVE-2008-0067
10.8.0.150	8059 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.150	80/tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.150	8082 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.150	5985 /tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.150	80/tcp	unsuccessful exploit	Oracle Endeca Server createDataStore method command execution	Other	CVE-2013-3763
10.8.0.150	8082 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.150	5985 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.150	80/tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.150	8059 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.150	80/tcp	unsuccessful exploit	PHP Remote File Inclusion	Web	
10.8.0.150	80/tcp	unsuccessful exploit	phpBB viewtopic.php highlight parameter vulnerability	Web	CVE-2005-2086
10.8.0.150	80/tcp	unsuccessful exploit	phpRPC decode function command execution	Web	CVE-2006-1032
10.8.0.150	8082 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.150	80/tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.150	8059 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.150	5985 /tcp	unsuccessful exploit	Plone Zope SAXutils Command Execution	Web	CVE-2011-3587
10.8.0.150	80/tcp	unsuccessful exploit	RSA Authentication Agent for Web for IIS chunked encoding overflow	Web	CVE-2005-1471
10.8.0.150	8082 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.150	80/tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	SAP NetWeaver SAPHostControl Command Injection	Other	

10.8.0.150	8082 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.150	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.150	8082 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.150	80/tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.150	8082 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.150	5985 /tcp	unsuccessful exploit	Serv-U Web Client session cookie handling buffer overflow	Web	
10.8.0.150	80/tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.150	8059 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.150	5985 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.150	8082 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.150	80/tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.150	80/tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.150	8082 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.150	5985 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.150	8059 /tcp	unsuccessful exploit	Apache Struts DefaultActionMapper redirect Prefix Vulnerability	Web	CVE-2013-2251
10.8.0.150	80/tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.150	8082 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.150	5985 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.150	8059 /tcp	unsuccessful exploit	Apache Struts URL includeParams Attribute OGNL Code Injection	Web	CVE-2013-2115
10.8.0.150	80/tcp	unsuccessful exploit	Sun Java System Web Server WebDAV OPTIONS request buffer overflow	Web	CVE-2010-0361
10.8.0.150	8082 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.150	5985 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014
10.8.0.150	8059 /tcp	unsuccessful exploit	Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities	Web	CVE-2013-5014

10.8.0.150	69/udp	unsuccessful exploit	TFTP Server error packet buffer overflow	File Transfer	CVE-2008-2161
10.8.0.150	8059 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.150	80/tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.150	5985 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.150	8082 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.150	80/tcp	unsuccessful exploit	Traq authenticate function remote code execution	Web	
10.8.0.150	8059 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.150	5985 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.150	80/tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.150	8082 /tcp	unsuccessful exploit	Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow	Web	CVE-2008-2437
10.8.0.150	5985 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.150	8082 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.150	8059 /tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.150	80/tcp	unsuccessful exploit	Trend Micro OfficeScan Policy Server CGI buffer overflow	Web	CVE-2008-1365
10.8.0.150	5985 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.150	8082 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.150	8059 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.150	80/tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.150	8059 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.150	8082 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.150	80/tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.150	5985 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.150	8059 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.150	8082 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.150	80/tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.150	5985 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.150	8059 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.150	80/tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.150	8082 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214

10.8.0.150	5985 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.150	5985 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.150	8082 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.150	80/tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.150	8059 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.150	80/tcp	unsuccessful exploit	Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow	Web	CVE-2008-4008
10.8.0.150	80/tcp	unsuccessful exploit	WhatsUp Gold _maincfgret.cgi instancename buffer overflow	Web	CVE-2004-0798
10.8.0.150	445 /tcp	unsuccessful exploit	Windows Plug and Play buffer overflow	Windows OS	CVE-2005-1983
10.8.0.150	445 /tcp	unsuccessful exploit	Windows Workstation service NetpManageIPCConnect buffer overflow	Windows OS	CVE-2006-4691
10.8.0.150		unsuccessful exploit	Wireshark DECT Dissector Remote Stack Buffer Overflow	Other	CVE-2011-1591
10.8.0.150	8082 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.150	8059 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.150	5985 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.150	80/tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.150	80/tcp	unsuccessful exploit	Xi Software Net Transport eDonkey Protocol Buffer Overflow	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.150	80/tcp	unsuccessful exploit	Novell ZENworks Asset Management File Upload Traversal	Other	CVE-2010-4229
10.8.0.150	80/tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell ZENworks Asset Management rtrlet File Upload Traversal	Web	CVE-2011-2653
10.8.0.150	80/tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell ZENworks Configuration Management UploadServlet Remote Code Execution	Other	
10.8.0.150	80/tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082

10.8.0.150	5985 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability	Other	CVE-2013-1082
10.8.0.150	5985 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.150	8059 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.150	8082 /tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.150	80/tcp	unsuccessful exploit	Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability	Other	CVE-2013-1081
10.8.0.150	1026 /tcp	service	1026/TCP		
10.8.0.150	1027 /tcp	service	1027/TCP		
10.8.0.150	1029 /tcp	service	1029/TCP		
10.8.0.150	1033 /tcp	service	1033/TCP		
10.8.0.150	1039 /tcp	service	1039/TCP		
10.8.0.150	1044 /tcp	service	1044/TCP		
10.8.0.150	9389 /tcp	service	9389/TCP		
10.8.0.150	53/tcp	service	DNS		
10.8.0.150		service	NFS		
10.8.0.150	139 /tcp	service	SMB		
10.8.0.150	80/tcp	service	WWW		
10.8.0.150	443 /tcp	service	WWW (Secure)		
10.8.0.150	5985 /tcp	service	WWW (non-standard port 5985)		
10.8.0.150	8059 /tcp	service	WWW (non-standard port 8059)		
10.8.0.150	8082 /tcp	service	WWW (non-standard port 8082)		
10.8.0.150	1025 /tcp	service	blackjack (1025/TCP)		
10.8.0.150	1050 /tcp	service	cma (1050/TCP)		
10.8.0.150	53/udp	service	domain (53/UDP)		
10.8.0.150	135 /tcp	service	epmap (135/TCP)		
10.8.0.150	593 /tcp	service	http-rpc-epmap (593/TCP)		
10.8.0.150	1030 /tcp	service	iad1 (1030/TCP)		
10.8.0.150	1031 /tcp	service	iad2 (1031/TCP)		
10.8.0.150	3260 /tcp	service	iscsi-target (3260/TCP)		
10.8.0.150	88/tcp	service	kerberos (88/TCP)		
10.8.0.150	464 /tcp	service	kpasswd (464/TCP)		

10.8.0.150	389 /tcp	service	ldap (389/TCP)
10.8.0.150	4345 /tcp	service	m4-network-as (4345/TCP)
10.8.0.150	445 /tcp	service	microsoft-ds (445/TCP)
10.8.0.150	3389 /tcp	service	ms-wbt-server (3389/TCP)
10.8.0.150	3268 /tcp	service	msft-gc (3268/TCP)
10.8.0.150	3269 /tcp	service	msft-gc-ssl (3269/TCP)
10.8.0.150	1047 /tcp	service	neod1 (1047/TCP)
10.8.0.150	1048 /tcp	service	neod2 (1048/TCP)
10.8.0.150	137 /udp	service	netbios-ns (137/UDP)
10.8.0.150	1092 /tcp	service	obrpd (1092/TCP)
10.8.0.150	1093 /tcp	service	proofd (1093/TCP)
10.8.0.150	2049 /tcp	service	shilp (2049/TCP)
10.8.0.150	636 /tcp	service	ssl-ldap (636/TCP)
10.8.0.150	111 /tcp	service	sunrpc (111/TCP)
10.8.0.150	69/udp	service	tftp (69/UDP)
10.8.0.150	4343 /tcp	service	unicall (4343/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100000-2 portmapper (111/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100000-2 portmapper (111/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100000-3 portmapper (111/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100000-3 portmapper (111/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100000-4 portmapper (111/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100000-4 portmapper (111/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100003-2 nfs (2049/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100003-2 nfs (2049/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100003-3 nfs (2049/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100003-3 nfs (2049/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100005-1 mountd (1048/TCP)
10.8.0.150	111 /tcp	info	RPC service: 100005-1 mountd (1048/UDP)
10.8.0.150	111 /tcp	info	RPC service: 100005-2 mountd (1048/TCP)

10.8.0.150	111 /tcp	info	RPC service: 100005-2 mountd (1048/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100005-3 mountd (1048/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100005-3 mountd (1048/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-1 nlockmgr (1047/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-1 nlockmgr (1047/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-2 nlockmgr (1047/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-2 nlockmgr (1047/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-3 nlockmgr (1047/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-3 nlockmgr (1047/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-4 nlockmgr (1047/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100021-4 nlockmgr (1047/UDP)		
10.8.0.150	111 /tcp	info	RPC service: 100024-1 status (1039/TCP)		
10.8.0.150	111 /tcp	info	RPC service: 100024-1 status (1039/UDP)		
10.8.0.230	139 /tcp	remote admin	Windows password weakness (nobody:)	Passwords	CVE-1999-0503
10.8.0.230	8834 /tcp	unsuccessful exploit	ALCASAR index.php Crafted HTTP host Header Vulnerability	Web	
10.8.0.230	8834 /tcp	unsuccessful exploit	AWStats migrate parameter command injection	Web	CVE-2006-2237
10.8.0.230	8834 /tcp	unsuccessful exploit	BASE base_qry_common.php file include	Web	CVE-2006-2685
10.8.0.230	8834 /tcp	unsuccessful exploit	Bash environment variable code injection over HTTP	Web	CVE-2014-6271
10.8.0.230	8834 /tcp	unsuccessful exploit	Cisco IOS HTTP exec path command execution	Web	CVE-2000-0945
10.8.0.230	8834 /tcp	unsuccessful exploit	Cisco IOS HTTP access level authentication bypass	Web	CVE-2001-0537
10.8.0.230	8834 /tcp	unsuccessful exploit	CS-MARS JBoss jmx-console access	Web	CVE-2006-3733
10.8.0.230	8834 /tcp	unsuccessful exploit	D-Link Cookie command injection	Web	
10.8.0.230	8834 /tcp	unsuccessful exploit	JRun mod_jrun WriteToLog buffer overflow	Web	CVE-2004-0646
10.8.0.230	8834 /tcp	unsuccessful exploit	Nagios statuswml.cgi Command Injection	Web	CVE-2009-2288
10.8.0.230	8834 /tcp	unsuccessful exploit	Nagios XI Graph Explorer Component OS Command Injection Vulnerability	Other	
10.8.0.230	8834 /tcp	unsuccessful exploit	Nagios 3 history.cgi Command Injection	Web	CVE-2012-6096
10.8.0.230	8834 /tcp	unsuccessful exploit	PHP CGI Query String Parameters Command Execution	Web	CVE-2012-1823
10.8.0.230	8834 /tcp	unsuccessful exploit	phpMyAdmin preg_replace from_prefix sanitization vulnerability	Web	CVE-2013-3238
10.8.0.230	8834 /tcp	unsuccessful exploit	PineApp Mail-SeCure ldapsyncnow.php command injection	Web	

10.8.0.230	8834 /tcp	unsuccessful exploit	PineApp Mail-SeCure test_li_connection.php Command Injection	Web	
10.8.0.230	139 /tcp	unsuccessful exploit	Samba call_trans2open buffer overflow	Other	CVE-2003-0201
10.8.0.230	445 /tcp	unsuccessful exploit	Samba lsa_io_trans_names buffer overflow	Other	CVE-2007-2446
10.8.0.230	8834 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution	Other	
10.8.0.230	8834 /tcp	unsuccessful exploit	SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution	Other	
10.8.0.230	3133 /udp	unsuccessful exploit	Snort Back Orifice Pre-Processor buffer overflow	Other	CVE-2005-3252
10.8.0.230	445 /tcp	unsuccessful exploit	Snort DCE/RPC preprocessor buffer overflow	Other	CVE-2006-5276
10.8.0.230	8834 /tcp	unsuccessful exploit	SonicWall Multiple Products skipSessionCheck Authentication Bypass	Other	CVE-2013-1359
10.8.0.230	8834 /tcp	unsuccessful exploit	Splunk Search Jobs Remote Code Execution	Web	CVE-2011-4642
10.8.0.230	22/tcp	unsuccessful exploit	F5 BIG-IP SSH private key	Other	CVE-2012-1493
10.8.0.230	22/tcp	unsuccessful exploit	Symantec Messaging Gateway Default SSH Password	Passwords	CVE-2012-3579
10.8.0.230	8834 /tcp	unsuccessful exploit	Symantec Web Gateway access_log PHP Injection	Web	CVE-2012-0297
10.8.0.230	8834 /tcp	unsuccessful exploit	Symantec Web Gateway pbcontrol.php Command Injection	Web	CVE-2012-2953
10.8.0.230	8834 /tcp	unsuccessful exploit	TikiWiki file upload vulnerability (jhot.php)	Web	CVE-2006-4602
10.8.0.230	8834 /tcp	unsuccessful exploit	TWiki revision control shell command injection	Web	CVE-2005-2877
10.8.0.230	8834 /tcp	unsuccessful exploit	TWiki Search.pm shell command injection	Web	CVE-2004-1037
10.8.0.230	8834 /tcp	unsuccessful exploit	TWiki View Script debugenableplugins Request Parameter Vulnerability	Web	CVE-2014-7236
10.8.0.230	8834 /tcp	unsuccessful exploit	vTiger CRM AddEmailAttachment arbitrary file upload	Web	CVE-2013-3214
10.8.0.230	8834 /tcp	unsuccessful exploit	WebCalendar Pre-Auth PHP Code Execution	Web	CVE-2012-1495
10.8.0.230	8834 /tcp	unsuccessful exploit	WP Symposium Plugin for WordPress Arbitrary File Upload	Web	CVE-2014-10021
10.8.0.230	53/udp	service	DNS		
10.8.0.230	139 /tcp	service	SMB		
10.8.0.230	22/tcp	service	SSH		
10.8.0.230	8834 /tcp	service	WWW (non-standard port 8834)		
10.8.0.230	705 /tcp	service	agentx (705/TCP)		
10.8.0.230	445 /tcp	service	microsoft-ds (445/TCP)		
10.8.0.230	137 /udp	service	netbios-ns (137/UDP)		
10.8.0.230	111 /tcp	service	sunrpc (111/TCP)		
10.8.0.230	69/udp	service	tftp (69/UDP)		
10.8.0.230	111 /tcp	info	RPC service: 100000-2 portmapper (111/TCP)		

10.8.0.230	111 /tcp	info	RPC service: 100000-2 portmapper (111/UDP)
10.8.0.230	111 /tcp	info	RPC service: 100000-3 portmapper (111/TCP)
10.8.0.230	111 /tcp	info	RPC service: 100000-3 portmapper (111/UDP)
10.8.0.230	111 /tcp	info	RPC service: 100000-4 portmapper (111/TCP)
10.8.0.230	111 /tcp	info	RPC service: 100000-4 portmapper (111/UDP)
10.8.0.230	111 /tcp	info	RPC service: 100007-1 ypbind (704/UDP)
10.8.0.230	111 /tcp	info	RPC service: 100007-1 ypbind (705/TCP)
10.8.0.230	111 /tcp	info	RPC service: 100007-2 ypbind (704/UDP)
10.8.0.230	111 /tcp	info	RPC service: 100007-2 ypbind (705/TCP)
10.8.0.230	111 /tcp	info	RPC service: 100024-1 status (45037/TCP)
10.8.0.230	111 /tcp	info	RPC service: 100024-1 status (56106/UDP)
10.8.0.230	22/tcp	info	User: avahi
10.8.0.230	22/tcp	info	User: backup
10.8.0.230	22/tcp	info	User: bin
10.8.0.230	22/tcp	info	User: colord
10.8.0.230	22/tcp	info	User: daemon
10.8.0.230	22/tcp	info	User: dnsmasq
10.8.0.230	22/tcp	info	User: games
10.8.0.230	22/tcp	info	User: gdm
10.8.0.230	22/tcp	info	User: gnats
10.8.0.230	22/tcp	info	User: irc
10.8.0.230	22/tcp	info	User: libuuid
10.8.0.230	22/tcp	info	User: list
10.8.0.230	22/tcp	info	User: lp
10.8.0.230	22/tcp	info	User: mail
10.8.0.230	22/tcp	info	User: man
10.8.0.230	22/tcp	info	User: messagebus
10.8.0.230	22/tcp	info	User: mysql
10.8.0.230	22/tcp	info	User: news
10.8.0.230	22/tcp	info	User: nobody
10.8.0.230	22/tcp	info	User: proxy
10.8.0.230	22/tcp	info	User: pulse
10.8.0.230	22/tcp	info	User: root
10.8.0.230	22/tcp	info	User: rtkit
10.8.0.230	22/tcp	info	User: saint
10.8.0.230	22/tcp	info	User: saned
10.8.0.230	22/tcp	info	User: sshd
10.8.0.230	22/tcp	info	User: statd
10.8.0.230	22/tcp	info	User: sync
10.8.0.230	22/tcp	info	User: sys
10.8.0.230	22/tcp	info	User: syslog
10.8.0.230	22/tcp	info	User: testadmin
10.8.0.230	22/tcp	info	User: usbmux
10.8.0.230	22/tcp	info	User: uucp
10.8.0.230	22/tcp	info	User: www-data

4 Details

The following sections provide details on the specific exploits executed on each host.

4.1 10.8.0.14

IP Address: 10.8.0.14
Scan time: Dec 14 12:50:21 2015
Host type: Windows XP SP2
Netbios Name: XPPROUNPATCHED

Windows password weakness (Guest:)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight characters long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (HelpAssistant:)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (HelpServicesGroup:)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (SUPPORT_388945a0:)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (testadmin:testadmin)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the

system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

3Com TFTP server Transporting Mode buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-6183

Background

3CTftpSvc by 3Com is a freeware implementation of the TFTP protocol for Windows.

Problem

A buffer overflow vulnerability in the 3Com TFTP server allows remote attackers to execute arbitrary commands by sending a long, specially crafted transporting mode in a GET or PUT request.

Resolution

Delete the 3Com TFTP server. It is no longer supported by the vendor.

References

http://www.securityfocus.com/archive/1/452754

Limitations

Exploit works on 3Com TFTP server 2.0.1.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Apache mod_rewrite LDAP URL buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3747

Background

mod_rewrite is an Apache module which allows rule-based modification of URL requests.

Problem

An off-by-one buffer overflow vulnerability in mod_rewrite allows command execution when the **`escape_absolute_uri`** function attempts to separate tokens within an LDAP URL.

Resolution

Upgrade to Apache HTTP Server version 1.3.37, 2.0.59, or 2.2.3 or higher.

References

http://archives.neohapsis.com/archives/bugtraq/2006-07/0514.html
http://www.kb.cert.org/vuls/id/395412

Limitations

Exploit works on Apache HTTP Server 2.0.58. The vulnerability is only exploitable when there exists a rule where the user can control the initial part of the rewritten URL. The rule must not contain a forbidden or gone flag [F or G] or the "noescape" [NE] flag.

AWStats configdir parameter command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2005-0116

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

Insufficient validation of the **`configdir`** parameter before being used in a PERL open call leads to remote command execution.

Resolution

Upgrade to AWStats 6.3 or higher.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=185&type=vulnerabilities

Limitations

Exploit works on AWStats 6.2 on Linux.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **`base_qry_common.php`** script can be used to include arbitrary files under the directory specified by the **`BASE_path`** parameter. This could lead to execution of local

or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute

arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially

crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker

could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with

EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

GitList blame resource command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4511

Background

GitList is a web-based git repository viewer.

Problem

A vulnerability in GitList allows remote attackers to execute arbitrary commands by sending a specially crafted request for the **`blame`** resource.

Resolution

Upgrade to GitList 0.5.0 or higher.

References

http://hatriot.github.io/blog/2014/06/29/gitlist-rce/

Limitations

The URL path to a gitlist repository must be known.

Hastymail rs parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4542

Background

Hastymail is a fast, secure, rfc-compliant, cross-platform IMAP/SMTP client application written in PHP providing a clean web interface for sending and reading E-mail.

Problem

Hastymail2 fails to properly sanitize user-supplied input passed to rs and rsargs[] parameters to the default URI. This can be exploited to execute arbitrary commands.

Resolution

Upgrade to Hastymail2 2.1.1-RC2 or later.

References

https://www.dognaedis.com/vulns/DGS-SEC-3.html

Limitations

This exploit has been tested against Hastymail2 2.1.0 on Windows XP SP3 and Hastymail2 2.1.1-RC1 on Ubuntu 10.04 Linux.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated,

the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of

distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IIS Double Decoding Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0333

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by URL-encoding invalid characters twice. Thus, a backslash is first represented as %5c, and then %255c. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 01-026.

References

http://archives.neohapsis.com/archives/bugtraq/2001-05/0101.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

IIS Unicode Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0884

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by encoding invalid characters in Unicode. For example, a slash character is represented as %c0%af. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 00-078.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0263.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

JRun mod_jrun WriteToLog buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0646

Background

Macromedia JRun is a J2EE application server. mod_jrun is an Apache module which enables the use of JRun applications through an Apache web server.

Problem

A buffer overflow vulnerability in mod_jrun and mod_jrun20 allows a remote attacker to execute arbitrary commands on the web server if verbose logging is enabled.

Resolution

Apply the patch referenced in Macromedia Security Bulletin 04-08.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=145&type=vulnerabilities

Limitations

Exploit works on JRun 4 SP1a with verbose logging enabled.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2009-1350

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

A vulnerability in the **`xtagent.exe`** program allows remote, authenticated attackers to execute arbitrary commands by sending a specially crafted RPC message to the XTIERRPCPIPE named pipe which dereferences an arbitrary pointer.

Resolution

Apply the Novell NetIdentity 1.2.4 patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

Limitations

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

Novell Client nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5854

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflows in the **`EnumPrinters`** and **`OpenPrinter`** functions, allowing remote attackers to execute arbitrary commands by sending a specially

crafted RPC request to the Spooler service.

Resolution

Apply **`491psp3_nwspool.exe`**. Patches are available from Novell.

References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***`%windir%`*`\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<`*`computername`*`>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`nnmRptConfig.exe`** CGI program with a long, specially crafted **`Template`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`nnmRptConfig.exe`** CGI program with a specially crafted **`nameParams/text1`** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **OpenView5.exe** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **ovalarm.exe** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows

Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **`act`** and **`app`** parameters to the **`snmpviewer.exe`** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **`Read`** and **`Execute`** privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note

that users in the groups **`Users`** and **`Power Users`** don't have those privileges, but users in the groups **`Administrators`** and **`TelnetClients`** do.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

PHP Remote File Inclusion

Severity: Unsuccessful Exploit

Background

PHP scripts support the **`include`** and **`require`** statements, which cause an outside script to be run within the calling script. The included script can be a local file or, in some configurations, the URL of a remote file.

Problem

The PHP script is vulnerable to a remote file inclusion vulnerability. This vulnerability typically arises due to an **`include`** or **`require`** command where the included file path can be manipulated by a remote user via a specific HTTP input parameter. A remote attacker could execute arbitrary PHP commands on the target by specifying the URL of a PHP script on his or her own server in the input parameter.

Resolution

Fix the vulnerable code so that included path names cannot be manipulated by the user.

The vulnerability can also be mitigated by setting the following variables in the PHP configuration file:

```
register_globals = Off
allow_url_include = Off
safe_mode = On
```

References

http://projects.webappsec.org/Remote-File-Inclusion

Limitations

This exploit works against Unix and Linux operating systems.

The exploit requires the **register_globals** and **allow_url_include** PHP settings to be on, and the **safe_mode** PHP setting to be off.

The **telnet** and **mkfifo** programs must exist on the target in order for the shell connection to be established.

phpBB viewtopic.php highlight parameter vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2086

Background

phpBB is an open-source bulletin board package written in PHP.

Problem

This is a variant of an older vulnerability which allows remote command execution by requesting **viewtopic.php** with a specially crafted **highlight** parameter.

Resolution

Upgrade to the latest version of phpBB.

References

http://archives.neohapsis.com/archives/bugtraq/2005-06/0256.html

phpRPC decode function command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2006-1032

Background

phpRPC is an xmlrpc library written in PHP supporting most databases.

Problem

A vulnerability in the **decode** function allows a remote attacker to execute arbitrary PHP commands placed inside a **<base64>** tag.

Resolution

phpRPC is no longer maintained by the author, so no fix is available. If phpRPC is installed as part of another product, contact the vendor of that product for a fix. Otherwise, remove phpRPC from the server.

References

http://archives.neohapsis.com/archives/bugtraq/2006-02/0507.html

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

RSA Authentication Agent for Web for IIS chunked encoding overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1471

Background

RSA Authentication Agent For Web for IIS provides access control for applications on IIS web servers.

Problem

A heap overflow vulnerability when using chunked transfer-encoding allows remote attackers to execute arbitrary commands with LocalSystem privileges.

Resolution

A fix is available from https://knowledge.rsasecurity.com.

References

http://www.kb.cert.org/vuls/id/790533
http://archives.neohapsis.com/archives/vulnwatch/2005-q2/0039.html

Limitations

Exploit works on RSA Authentication Agent For Web for IIS 5.3 on Windows 2000 SP4.

The success of this exploit depends on the system state at the time the exploit is attempted.

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Snort Back Orifice Pre-Processor buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-3252

Background

Back Orifice is a remote system administration program for Windows. It is commonly installed by attackers or Trojan Horse programs for use as a backdoor.

Snort is an open-source intrusion detection system. It includes a Back Orifice pre-processor, which handles Back Orifice traffic before it is passed to the intrusion detection engine.

Problem

A buffer overflow vulnerability in the Back Orifice pre-processor in Snort could allow remote attackers to execute arbitrary commands by sending a specially crafted Back Orifice ping to a host on a network monitored by Snort.

Resolution

Upgrade to Snort 2.4.3 or higher.

References

http://www.kb.cert.org/vuls/id/175500

Limitations

Exploit works on Snort 2.4.2 on Windows and Red Hat 8.

Snort DCE/RPC preprocessor buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5276

Background

Snort is an open-source intrusion detection system. It includes a DCE/RPC preprocessor, which reassembles DCE/RPC traffic before it is passed to the intrusion detection engine.

Problem

A buffer overflow vulnerability in the DCE/RPC preprocessor allows remote attackers to execute arbitrary commands by chaining together multiple **`WriteAndX`** requests in the same TCP segment.

Resolution

Upgrade to Snort 2.6.1.3 or higher.

References

http://www.us-cert.gov/cas/techalerts/TA07-050A.html
http://www.snort.org/docs/advisory-2007-02-19.html

Limitations

Exploit works on Snort 2.6.1.1 on Windows and Snort 2.6.1.2 on Red Hat 8, and requires port 445/TCP to be open on the target.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Sun Java System Web Server WebDAV OPTIONS request buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0361

Background

Sun Java System Web Server is a web application server. WebDAV (Web-based Distributed Authoring and Versioning) is an extension to the HTTP protocol which allows users to edit web server content.

Problem

A buffer overflow vulnerability in Sun Java System Web Server's WebDAV implementation allows remote attackers to execute arbitrary commands by sending a specially crafted OPTIONS request.

Resolution

Upgrade to Sun Java System Web Server 6.1 Service Pack 12 or 7.0 Release 8 or higher.

References

http://secunia.com/advisories/38260/
http://sunsolve.sun.com/search/document.do?assetkey=1-66-275850-1

Limitations

Exploit works on Sun Java System Web Server 7.0 Update 7 on Windows Server 2003 SP2 with patch KB933729.

WebDAV support must be enabled on the target in order for the exploit to succeed, and the correct WebDAV URI must be specified.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Traq authenticate function remote code execution

Severity: Unsuccessful Exploit

Background

Traq is a PHP5+ and MySQL4+ based Project Tracking system with the ability to host multiple projects.

Problem

The flaw is caused due to admin rights not properly being restricted in the "authenticate()" function in admincp /common.php. This can be exploited to execute arbitrary code.

Resolution

Upgrade to Traq 2.3.1 or later.

References

http://www.exploit-db.com/exploits/18213
http://secunia.com/advisories/47108

Limitations

This exploit has been tested against Traq 2.3 on Linux.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **`pwd`** parameter to the **`cgiABLogon.exe`** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4008

Background

Oracle WebLogic Server (formerly BEA WebLogic Server) is a Java web application platform.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted Transfer-Encoding header in an HTTP request.

Resolution

Install the latest WebLogic Server plug-in referenced in the Oracle Security Advisory.

References

https://support.bea.com/application_content/product_portlets/securityadvisories/2806.html

Limitations

Exploit works on the WebLogic Server Connector for Apache 1.0.1136334.

WhatsUp Gold _maincfgret.cgi instancename buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0798

Background

WhatsUp Professional (formerly WhatsUp Gold) is a network mapping and monitoring tool.

Problem

A buffer overflow in the WhatsUp Gold web interface allows remote command execution by requesting **`_maincfgret.cgi`** with a long **`instancename`** parameter.

Resolution

Install WhatsUp Gold 8.03 Hotfix 1.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=133&type=vulnerabilities

Limitations

Exploit works on Ipswitch WhatsUp Gold 8.03.

Successful exploitation requires valid user credentials with permissions to *Configure Program* and *Configure Reports*.

Note that the WhatsUp Gold installation path may affect the success of this exploit. The exploit is designed to work with the default installation path only.

Windows LSASS buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0533

Background

The Local Security Authority Subsystem Service (LSASS) provides an interface for managing local security, domain authentication, and Active Directory processes.

Problem

A buffer overflow in the **`DsRolepInitializeLog`** function in the Windows LSASS service allows remote command execution.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 04-011.

References

http://www.kb.cert.org/vuls/id/753212

Limitations

This exploit may cause the target system to crash.

Windows Plug and Play buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1983

Background

The Windows Plug and Play service allows Windows operating systems to automatically detect and configure a new hardware device, such as a mouse.

Problem

A buffer overflow in the Plug and Play service could allow command execution with administrative privileges.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 05-047.

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Limitations

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

Windows Server Service buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3439

Background

The Windows Server Service supports file, print, and named-pipe sharing over the network.

Problem

A buffer overflow vulnerability in the Windows Server Service allows remote attackers to execute arbitrary commands.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 06-040.

References

http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

Limitations

Exploit works on Windows 2000 and Windows XP SP1. Target computer may reboot after connection is closed.

Windows Server Service buffer overflow MS08-067

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4250

Background

The Windows Server service supports file, print, and named-pipe sharing over the network.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Windows Server service.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 08-067.

References

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

Limitations

Due to the nature of this vulnerability, the success of the exploit depends on the contents of unused stack memory space, and therefore is not completely reliable.

Windows Workstation service NetpManageIPCConnect buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4691

Background

The Windows Workstation service routes network requests for file or printer resources.

Problem

A buffer overflow in the NetpManageIPCConnect function in the Windows Workstation service allows command execution when a domain join request causes communication with a malicious domain controller.

Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

Wireshark DECT Dissector Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-1591

Background

Wireshark is a network packet analyzer.

Problem

A buffer overflow vulnerability in the DECT dissector allows command execution when a user sends a specially crafted datagram over a network which is being analyzed by Wireshark.

Resolution

Upgrade to Wireshark 1.4.5 or higher.

References

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Limitations

Exploit works on Wireshark 1.4.4.

The affected target running Wireshark must be on the same network as as the SAINTexploit host.

Exploit requires the Net-Write PERL module to be installed on the scanning host. This module is available from http://search.cpan.org/dist/Net-Write/lib/Net/Write.pm.

The "Wireshark DECT Dissector PCAP File Processing Overflow" client exploit attempts to exploit the same vulnerability. The client exploit does not have the same network and PERL module limitations, but requires user cooperation.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

Xi Software Net Transport eDonkey Protocol Buffer Overflow

Severity: Unsuccessful Exploit

Background

Net Transport, also known as NetXfer, is a download manager for Windows made by Xi Software. Among the protocols Net Transport can handle is eDonkey, a decentrailized peer to peer network for file sharing.

Problem

The Net Transport download manager fails to properly sanitize user input from the eDonkey network, specifically in processing eDonkey **`OP_LOGINREQUEST`** packets. A successful attacker sending a specially crafted packet could cause a stack buffer overflow and execute arbitrary code.

Resolution

Restrict access to the port used for eDonkey. Upgrade to a newer version of Net Transport that contains a fix.

References

http://secunia.com/advisories/38028/

Limitations

Exploit runs on Xi Software Net Transport 2.90.510.
The eDonkey service port must be known by the attacker. By default, the application uses a random port.
The exploit may take a longer time to establish a shell connection.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

1026/UDP

Severity: Service

DNS

Severity: Service

SMB

Severity: Service

WWW

Severity: Service

XDM (X login)

Severity: Service

blackjack (1025/UDP)

Severity: Service

epmap (135/TCP)

Severity: Service

h323gatedisc (1718/UDP)

Severity: Service

h323gatestat (1719/UDP)

Severity: Service

isakmp (500/UDP)

Severity: Service

microsoft-ds (445/TCP)

Severity: Service

microsoft-ds (445/UDP)

Severity: Service

ms-wbt-server (3389/TCP)

Severity: Service

netbios-dgm (138/UDP)

Severity: Service

netbios-ns (137/UDP)

Severity: Service

ntp (123/UDP)

Severity: Service

ssdp (1900/UDP)

Severity: Service

tftp (69/UDP)

Severity: Service

4.2 10.8.0.20

IP Address: 10.8.0.20
Scan time: Dec 14 12:47:23 2015

Host type: Windows 8.1
Netbios Name: WIN81

Windows password weakness (testadmin:testadmin)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **migrate** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **AllowToUpdateStatsFromBrowser** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to

authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can

leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of

distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid

user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`nnmRptConfig.exe`** CGI program with a specially crafted **`nameParams/text1`** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and

usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04

Linux.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

TFTP Server error packet buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2161

Background

TFTP Server is an open source server implementation of the tftp protocol for multiple platforms.

Problem

A buffer overflow vulnerability in the handling of error packets allows remote attackers to execute arbitrary commands.

Resolution

Upgrade to version 1.6 or higher when available, if that version contains a fix. Otherwise restrict access to the tftp service.

References

http://www.milw0rm.com/exploits/5563

Limitations

Exploit works on TFTP Server SP 1.4.

A different payload is required depending upon whether the service runs as a network service or standalone. Choose the first platform if TFTP Server is running as a network service, and the second if it is running standalone.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **`pwd`** parameter to the **`cgiABLogon.exe`** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Windows Plug and Play buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1983

Background

The Windows Plug and Play service allows Windows operating systems to automatically detect and configure a new hardware device, such as a mouse.

Problem

A buffer overflow in the Plug and Play service could allow command execution with administrative privileges.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 05-047.

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Limitations

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

Windows Workstation service NetpManageIPCConnect buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4691

Background

The Windows Workstation service routes network requests for file or printer resources.

Problem

A buffer overflow in the NetpManageIPCConnect function in the Windows Workstation service allows command execution when a domain join request causes communication with a malicious domain controller.

Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

Wireshark DECT Dissector Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-1591

Background

Wireshark is a network packet analyzer.

Problem

A buffer overflow vulnerability in the DECT dissector allows command execution when a user sends a specially crafted datagram over a network which is being analyzed by Wireshark.

Resolution

Upgrade to Wireshark 1.4.5 or higher.

References

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Limitations

Exploit works on Wireshark 1.4.4.

The affected target running Wireshark must be on the same network as as the SAINTexploit host.

Exploit requires the Net-Write PERL module to be installed on the scanning host. This module is available from http://search.cpan.org/dist/Net-Write/lib/Net/Write.pm.

The "Wireshark DECT Dissector PCAP File Processing Overflow" client exploit attempts to exploit the same vulnerability. The client exploit does not have the same network and PERL module limitations, but requires user cooperation.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841

http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

2179/TCP

Severity: Service

DNS

Severity: Service

SMB

Severity: Service

WWW (non-standard port 5357)

Severity: Service

epmap (135/TCP)

Severity: Service

microsoft-ds (445/TCP)

Severity: Service

ms-wbt-server (3389/TCP)

Severity: Service

netbios-ns (137/UDP)

Severity: Service

tftp (69/UDP)

Severity: Service

4.3 10.8.0.38

IP Address: 10.8.0.38
Scan time: Dec 14 12:47:24 2015

Host type: Windows 7 SP1
Netbios Name: WIN7

Windows password weakness (testadmin:testadmin)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight characters long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **migrate** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **AllowToUpdateStatsFromBrowser** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy FTP Server MKD command buffer overflow

Severity: Unsuccessful Exploit

Background

UplusFTP (formerly Easy FTP Server) is a free FTP server for Windows platforms.

Problem

A buffer overflow vulnerability allows remote, authenticated attackers to execute arbitrary commands by sending a MKD command with a specially crafted argument.

Resolution

Upgrade to UplusFTP 1.7.1.0 or higher.

References

http://www.net-security.org/vuln.php?id=11092

Limitations

Exploit works on Easy FTP Server 1.7.0.2 on Windows Server 2003 SP2 with the patch KB933729.

This exploit requires valid FTP authentication credentials.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly

validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

Freefloat FTP Server USER Command Buffer Overflow

Severity: Unsuccessful Exploit

Background

Freefloat is a software series developed directly for handheld terminals. Freefloat FTP Server is a free FTP server for various versions of Windows including Windows CE/Pocket PC.

Problem

Freefloat FTP Server is vulnerable to a stack overflow as a result of sending overly long replies. The vulnerability can be triggered by the attacker by sending the FTP server a **USER** command with an overly long username parameter.

Resolution

Use a firewall to restrict access to trusted computers, install an update from the vendor when one becomes available, or choose another FTP server.

References

http://secunia.com/advisories/42465/

Limitations

Exploit works on Freefloat FTP Server 1.0 on Microsoft Windows Server 2003 SP2 with KB956802 and KB956572.

Freefloat FTPD Invalid Command Overflow

Severity: Unsuccessful Exploit

Background

Freefloat is a software series developed directly for handheld terminals. Freefloat FTP Server is a free FTP server for various versions of Windows including Windows CE/Pocket PC.

Problem

Freefloat FTP Server is vulnerable to a stack overflow as a result of sending overly long replies. The vulnerability can be triggered by the attacker by sending the FTP server an overly long unknown command.

Resolution

No update is available at this time. Use a firewall to restrict access to trusted computers, install an update from the vendor when one becomes available, or choose another FTP server.

References

http://secunia.com/advisories/42465

Limitations

This exploit has been tested against FreeFloat FTP Server 1.0 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5

to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-5289

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP POST requests. A successful remote attacker could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.securityfocus.com/archive/1/533150/30/270/threaded

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2 32-bit, Windows XP SP3 32-bit and Windows 7 32-bit and 64-bit.

Konica Minolta FTP Utility buffer overflow

Severity: Unsuccessful Exploit

Background

The Konica Minolta FTP Utility is an FTP server for Windows 98 through XP.

Problem

A vulnerability in the FTP Utility allows remote, unauthenticated attackers to execute arbitrary commands by sending a long, specially crafted argument to any command.

Resolution

Remove the Konica Minolta FTP Utility.

References

https://www.exploit-db.com/exploits/38252/

Limitations

Exploit works on Konica Minolta FTP Utility 1.0 on Windows XP SP3.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2009-1350

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

A vulnerability in the **`xtagent.exe`** program allows remote, authenticated attackers to execute arbitrary commands by sending a specially crafted RPC message to the XTIERRPCPIPE named pipe which dereferences an arbitrary pointer.

Resolution

Apply the Novell NetIdentity 1.2.4 patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

Limitations

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

Novell Client nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5854

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflows in the **`EnumPrinters`** and **`OpenPrinter`** functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Apply **`491psp3_nwspool.exe`**. Patches are available from Novell.

References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Open and Compact FTP Server Long Password Buffer Overflow

Severity: Unsuccessful Exploit

Background

Open and Compact FTP Server (Open-FTPD) is a Windows-based compact FTP server.

Problem

A buffer overflow vulnerability allows command execution as a result of an overly long password.

Resolution

Upgrade to a version newer than 1.2 when it becomes available, or use a different FTP server.

References

http://www.exploit-db.com/exploits/11742
http://www.expbase.com/Remote/1718.html

Limitations

Exploit works on Open and Compact FTP Server 1.2.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **jovgraph.exe** allows remote attackers to execute arbitrary commands by sending an overly long **displayWidth** option in the **arg** parameter to the **jovgraph.exe** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the

nnmRptConfig.exe CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **`act`** and **`app`** parameters to the **`snmpviewer.exe`** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **Toolbar.exe** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **Toolbar.exe** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Ricoh DC Software DL-10 FTP Server USER Remote Code Execution

Severity: Unsuccessful Exploit

Background

Various cameras (e.g. CX1-6, G700, G700SE) provided by Ricoh support transfering images to a PC over FTP. Ricoh supplies a small FTP server called SR-10 / Capftpd which enables users to transfer images from camera to computer.

Problem

The flaw is caused due to a boundary error in the SR10 FTP server when logging FTP commands. This can be exploited to cause a stack-based buffer overflow via long username sent to TCP port 21 but requires the "Log file name" option to be enabled (disabled by default).

Resolution

No updates which address this vulnerability are available at this time. Until an update is available, discontinue use of this software or limit access to the vulnerable service.

References

http://secunia.com/advisories/47912/
http://security.inshell.net/advisory/5

Limitations

This exploit has been tested against Ricoh SR10 FTP server 4.5.0.1 (SR10.exe 1.1.0.6) on Windows XP SP3 English (DEP OptIn).

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

TFTP Server error packet buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2161

Background

TFTP Server is an open source server implementation of the tftp protocol for multiple platforms.

Problem

A buffer overflow vulnerability in the handling of error packets allows remote attackers to execute arbitrary commands.

Resolution

Upgrade to version 1.6 or higher when available, if that version contains a fix. Otherwise restrict access to the tftp service.

References

http://www.milw0rm.com/exploits/5563

Limitations

Exploit works on TFTP Server SP 1.4.

A different payload is required depending upon whether the service runs as a network service or standalone. Choose the first platform if TFTP Server is running as a network service, and the second if it is running standalone.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **rev** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **rev** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **rev** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **rev** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Windows Plug and Play buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1983

Background

The Windows Plug and Play service allows Windows operating systems to automatically detect and configure a new hardware device, such as a mouse.

Problem

A buffer overflow in the Plug and Play service could allow command execution with administrative privileges.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 05-047.

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Limitations

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

Windows Workstation service NetpManageIPCConnect buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4691

Background

The Windows Workstation service routes network requests for file or printer resources.

Problem

A buffer overflow in the NetpManageIPCConnect function in the Windows Workstation service allows command execution when a domain join request causes communication with a malicious domain controller.

Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

Wireshark DECT Dissector Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-1591

Background

Wireshark is a network packet analyzer.

Problem

A buffer overflow vulnerability in the DECT dissector allows command execution when a user sends a specially crafted datagram over a network which is being analyzed by Wireshark.

Resolution

Upgrade to Wireshark 1.4.5 or higher.

References

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Limitations

Exploit works on Wireshark 1.4.4.

The affected target running Wireshark must be on the same network as as the SAINTexploit host.

Exploit requires the Net-Write PERL module to be installed on the scanning host. This module is available from http://search.cpan.org/dist/Net-Write/lib/Net/Write.pm.

The "Wireshark DECT Dissector PCAP File Processing Overflow" client exploit attempts to exploit the same vulnerability. The client exploit does not have the same network and PERL module limitations, but requires user cooperation.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WS_FTP MKD command buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1135

Background

WS_FTP Server is an FTP server for Windows platforms.

Problem

A buffer overflow vulnerability in the **`MKD`** command could allow an attacker to execute commands on the server. If the anonymous FTP account is enabled, the attacker would not need to know a valid login and password in order to exploit the vulnerability.

Resolution

Upgrade to WS_FTP Server 5.04 or higher.

References

http://archives.neohapsis.com/archives/fulldisclosure/2004-11/1330.html

Limitations

Exploit works on WS_FTP Server 5.03 and requires a valid FTP user name and password.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is

executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2

English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

1026/TCP

Severity: Service

1027/TCP

Severity: Service

1033/TCP

Severity: Service

DNS

Severity: Service

FTP

Severity: Service

SMB

Severity: Service

WWW (non-standard port 5357)

Severity: Service

WWW (non-standard port 5985)

Severity: Service

blackjack (1025/TCP)

Severity: Service

epmap (135/TCP)
Severity: Service

ftps (990/TCP)
Severity: Service

iad3 (1032/TCP)
Severity: Service

microsoft-ds (445/TCP)
Severity: Service

ms-wbt-server (3389/TCP)
Severity: Service

netbios-ns (137/UDP)
Severity: Service

startron (1057/TCP)
Severity: Service

tftp (69/UDP)
Severity: Service

4.4 10.8.0.46

IP Address: 10.8.0.46
Scan time: Dec 14 12:46:29 2015

Host type: Ubuntu 14.04
Netbios Name: SAINT84VM64

Windows password weakness (nobody:)
Severity: Remote Administrator **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for

invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **`base_qry_common.php`** script can be used to include arbitrary files under the directory specified by the **`BASE_path`** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://`*`target`*`/level/`*`xx`*`/exec/`*`command`***, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

F5 BIG-IP SSH private key

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1493

Background

SSH Private keys are used for authentication for many F5 BIG-IP devices. Devices shipped with a default, static key are vulnerable to compromise if the public discovers the key. The private key can be re-used by an attacker to gain remote, privileged access to the device.

Problem

Vulnerable BIG-IP installations allow unauthenticated users to bypass authentication and login as the 'root' user on the following devices:

- VIPRION B2100, B4100, and B4200
- BIG-IP 520, 540, 1000, 2000, 2400, 5000, 5100, 1600, 3600, 3900, 6900, 8900, 8950, 11000, and 11050
- BIG-IP Virtual Edition

- Enterprise Manager 3000 and 4000

Resolution

The vendor has indicated these versions are patched:

- 9.4.8-HF5 and later
- 10.2.4 and later
- 11.0.0-HF2 and later
- 11.1.0-HF3 and later

Note: Systems that are licensed to run in Appliance mode on BIG-IP version 10.2.1-HF3 or later are not susceptible to this vulnerability. For more information about Appliance mode, refer to SOL12815: Overview of Appliance mode.

References

http://support.f5.com/kb/en-us/solutions/public/12000/800/sol12815.html

Limitations

The target must be running the ssh service in order for the exploit to succeed.

The OpenSSH client must be installed on the SAINTexploit host.

Symantec Messaging Gateway Default SSH Password

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3579

Background

Symantec Messaging Gateway is an email virus protection appliance that also provides antispam protection.

Problem

Symantec Messaging Gateway versions before 10.0 have a default password for the "support" account, which can be used to login remotely to the SSH service, and then gain privileged access.

Resolution

Upgrade to Symantec Messaging Gateway 10.0 or higher.

References

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120827_00

Limitations

Exploit works against Symantec Messaging Gateway 9.5.3-3 on platform CentOS Project CentOS 5.0 with Exec-Shield Enabled.

The OpenSSH client must be installed on the SAINTexploit host.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

623/TCP

Severity: Service

DNS

Severity: Service

SMB

Severity: Service

SSH

Severity: Service

WWW (Secure)

Severity: Service

microsoft-ds (445/TCP)

Severity: Service

netbios-ns (137/UDP)

Severity: Service

sunrpc (111/TCP)

Severity: Service

tftp (69/UDP)

Severity: Service

4.5 10.8.0.101

IP Address: 10.8.0.101
Scan time: Dec 14 12:50:21 2015

Host type: Windows Server 2003 SP2
Netbios Name: WIN2003PATCHED

Smart Software Solutions CoDeSys Webserver URI Copying Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-5007

Background

Smart Software Solutions GmbH (3S) manufactures CoDeSys Web Server, a Supervisory Control and Data Acquisition/Human-Machine Interface (SCADA/HMI) product. The SCADA Web Server listens on TCP port 8080.

Problem

The **`CmpWebServer.dll`** library is affected by a buffer overflow in the function **`0040f480`** that copies the input URI into a limited stack buffer allowing code execution.

Resolution

Upgrade or apply patches when they become available.

References

http://aluigi.altervista.org/adv/codesys_1-adv.txt
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-336-01.pdf
http://www.scadahacker.com/vulndb/2011/ics-vuln-3s-11-336-01.html

Limitations

Exploit works on Smart Software Solutions CoDeSys 2.3.9.31, running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) with patches KB956802 and KB2393802 installed.

Smart Software Solutions CoDeSys Webserver URI Copying Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-5007

Background

Smart Software Solutions GmbH (3S) manufactures CoDeSys Web Server, a Supervisory Control and Data Acquisition/Human-Machine Interface (SCADA/HMI) product. The SCADA Web Server listens on TCP port 8080.

Problem

The **`CmpWebServer.dll`** library is affected by a buffer overflow in the function **`0040f480`** that copies the input URI into a limited stack buffer allowing code execution.

Resolution

Upgrade or apply patches when they become available.

References

http://aluigi.altervista.org/adv/codesys_1-adv.txt
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-336-01.pdf
http://www.scadahacker.com/vulndb/2011/ics-vuln-3s-11-336-01.html

Limitations

Exploit works on Smart Software Solutions CoDeSys 2.3.9.31, running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) with patches KB956802 and KB2393802 installed.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

Computer Associates Alert Notification Server buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-3825

Background

The Alert Notification Server is included with multiple Computer Associates products to provide notifications to console users.

Problem

The Alert Notification Server is affected by buffer overflow vulnerabilities in multiple RPC operations allowing remote attackers to execute arbitrary commands.

Resolution

Apply fix QO89817.

References

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=561
http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-secnotice.asp

Limitations

Exploit works on CA BrightStor ARCserve Backup 11.5 and requires a valid login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation. These packages are available from http://cpan.org/modules/by-module/.

Computer Associates Alert Notification Server opcode 23 buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-4620

Background

The Alert Notification Server is included with multiple Computer Associates products to provide notifications to console users.

Problem

The Alert Notification Server is affected by buffer overflow vulnerabilities in multiple RPC operations allowing remote attackers to execute arbitrary commands.

Resolution

Apply one of the updates referenced in the Security Notice.

References

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=679

Limitations

Exploit works on CA eTrust Antivirus r8 with patch QO89817. Valid Windows credentials are required in

order for this exploit to succeed.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco Secure ACS UCP CSuserCGI.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0532

Background

Cisco Secure Access Control Server (ACS) is a centralized user access control framework which can be used with routers, switches, firewalls, VPNs, and other devices. User Changeable Passwords (UCP), a utility implemented by Cisco Secure ACS, allows users to change their ACS passwords using a web browser.

Problem

A buffer overflow in the **`CSuserCGI.exe`** program allows remote attackers to execute arbitrary commands by sending a specially crafted HTTP request with a long Logout argument.

Resolution

Upgrade to UCP 4.2.

References

http://www.cisco.com/warp/public/707/cisco-sa-20080312-ucp.shtml
http://www.frsirt.com/english/advisories/2008/0868

Limitations

Exploit works on Cisco UCP 4.1.4.13.

On Windows Server 2003, Read and Execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account "IUSR_" for the exploit to work properly.

Cisco Secure ACS UCP CSuserCGI.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0532

Background

Cisco Secure Access Control Server (ACS) is a centralized user access control framework which can be used with routers, switches, firewalls, VPNs, and other devices. User Changeable Passwords (UCP), a utility implemented by Cisco Secure ACS, allows users to change their ACS passwords using a web browser.

Problem

A buffer overflow in the **`CSuserCGI.exe`** program allows remote attackers to execute arbitrary commands by sending a specially crafted HTTP request with a long Logout argument.

Resolution

Upgrade to UCP 4.2.

References

http://www.cisco.com/warp/public/707/cisco-sa-20080312-ucp.shtml
http://www.frsirt.com/english/advisories/2008/0868

Limitations

Exploit works on Cisco UCP 4.1.4.13.

On Windows Server 2003, Read and Execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account "IUSR_" for the exploit to work properly.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://`*`target`*`/level/`*`xx`*`/exec/`*`command`***, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server

uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

Free Download Manager Remote Control Server HTTP Authorization buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-0183

Background

Free Download Manager is a download accelerator and manager for Windows systems.

Problem

A buffer overflow vulnerability in the Free Download Manager Remote Control Server allows remote attackers to execute arbitrary commands by sending an HTTP request with a long, specially crafted Authorization header.

Resolution

Upgrade to version 3.0 build 848 or higher.

References

http://secunia.com/secunia_research/2009-3/

Limitations

Exploit works on Free Download Manager 3.0 Build 843.

On Windows Server 2003 targets, patch 933729 must be installed in order for the exploit to succeed.

Free Download Manager Remote Control Server HTTP Authorization buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-0183

Background

Free Download Manager is a download accelerator and manager for Windows systems.

Problem

A buffer overflow vulnerability in the Free Download Manager Remote Control Server allows remote attackers to execute arbitrary commands by sending an HTTP request with a long, specially crafted Authorization header.

Resolution

Upgrade to version 3.0 build 848 or higher.

References

http://secunia.com/secunia_research/2009-3/

Limitations

Exploit works on Free Download Manager 3.0 Build 843.

On Windows Server 2003 targets, patch 933729 must be installed in order for the exploit to succeed.

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded

request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be

executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a

browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications

and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring

applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls

for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

JRun mod_jrun WriteToLog buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0646

Background

Macromedia JRun is a J2EE application server. mod_jrun is an Apache module which enables the use of JRun applications through an Apache web server.

Problem

A buffer overflow vulnerability in mod_jrun and mod_jrun20 allows a remote attacker to execute arbitrary commands on the web server if verbose logging is enabled.

Resolution

Apply the patch referenced in Macromedia Security Bulletin 04-08.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=145&type=vulnerabilities

Limitations

Exploit works on JRun 4 SP1a with verbose logging enabled.

JRun mod_jrun WriteToLog buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0646

Background

Macromedia JRun is a J2EE application server. mod_jrun is an Apache module which enables the use of JRun applications through an Apache web server.

Problem

A buffer overflow vulnerability in mod_jrun and mod_jrun20 allows a remote attacker to execute arbitrary commands on the web server if verbose logging is enabled.

Resolution

Apply the patch referenced in Macromedia Security Bulletin 04-08.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=145&type=vulnerabilities

Limitations

Exploit works on JRun 4 SP1a with verbose logging enabled.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute

arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5854

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **nwspool.dll** library in Novell Client is affected by buffer overflows in the **EnumPrinters** and **OpenPrinter** functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Apply **491psp3_nwspool.exe**. Patches are available from Novell.

References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

Novell Client nwspool.dll EnumPrinters buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0639

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **nwspool.dll** library in Novell Client is affected by a buffer overflow in the **EnumPrinters** function, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Apply Novell Client 4.91 Post-SP2/3/4 nwspool.dll 2.

References

http://www.zerodayinitiative.com/advisories/ZDI-08-005.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4 with the 4.91 Post-SP2/3/4 nwspool.dll 1 patch.

In order for the exploit to succeed against Windows Server 2003 targets, a shared printer must be configured, the login and password of an account with administrator privileges must be provided, and the Crypt::DES, Digest::MD4, and Digest::MD5 PERL modules must be installed. These modules are available from http://cpan.org/modules/by-module/.

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***`%windir%`*`\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<`*`computername`*`>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<*computername*>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<*computername*>** for the exploit to work properly. Note that

users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager OvOSLocale cookie buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-0920

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a long, specially crafted OvOSLocale cookie in an HTTP request for Toolbar.exe.

Resolution

Apply one of the patches referenced in HPSBMA02416 SSRT090008.

References

http://www.securityfocus.com/archive/1/502054

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account (IUSR_<computername>) in order for the exploit to succeed. The 'Users' and 'Power Users' groups don't have such privileges, but the 'Administrators' and 'TelnetClients' groups can execute 'cmd.exe'.

The patch KB933729 must be applied on Windows Server 2003 in order to bypass DEP protection.

HP OpenView Network Node Manager OvOSLocale cookie buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-0920

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a long, specially crafted OvOSLocale cookie in an HTTP request for Toolbar.exe.

Resolution

Apply one of the patches referenced in HPSBMA02416 SSRT090008.

References

http://www.securityfocus.com/archive/1/502054

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account (IUSR_<computername>) in order for the exploit to succeed. The 'Users' and 'Power Users' groups don't have such privileges, but the 'Administrators' and 'TelnetClients' groups can execute 'cmd.exe'.

The patch KB933729 must be applied on Windows Server 2003 in order to bypass DEP protection.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **ovwebsnmpsrv.exe** allows remote attackers to execute arbitrary commands by sending specially crafted **sel** and **arg** parameters to the **jovgraph.exe** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil.dll stringToSeconds Buffer

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0262

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability affecting **ovwebsnmpsrv.exe**, in the **stringToSeconds** function in **ovutil.dll**, allows remote attackers to execute arbitrary commands by sending a specially crafted HTTP request.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-004/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil.dll stringToSeconds Buffer

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0262

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability affecting **ovwebsnmpsrv.exe**, in the **stringToSeconds** function in **ovutil.dll**, allows remote attackers to execute arbitrary commands by sending a specially crafted HTTP request.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-004/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **Toolbar.exe** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **Toolbar.exe** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Database Advanced Replication component DBMS_SNAP_INTERNAL overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-2116

Background

Package DBMS_SNAP_INTERNAL of schema SYS is an Advanced Replication component used internally by Oracle Database.

Problem

A buffer overflow vulnerability in DBMS_SNAP_INTERNAL allows remote attackers to execute arbitrary commands.

Resolution

Apply the Oracle Critical Patch Update for April 2007.

References

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Limitations

Exploit works on Oracle Database 10g 10.1.0.4 and requires the login and password of a valid database user with EXECUTE permission on package DBMS_SNAP_INTERNAL. (The default "scott" account does not have permission.)

Oracle Database Advanced Replication component DBMS_SNAP_INTERNAL overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-2116

Background

Package DBMS_SNAP_INTERNAL of schema SYS is an Advanced Replication component used internally by Oracle Database.

Problem

A buffer overflow vulnerability in DBMS_SNAP_INTERNAL allows remote attackers to execute arbitrary commands.

Resolution

Apply the Oracle Critical Patch Update for April 2007.

References

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Limitations

Exploit works on Oracle Database 10g 10.1.0.4 and requires the login and password of a valid database user with EXECUTE permission on package DBMS_SNAP_INTERNAL. (The default "scott" account does not have permission.)

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle password weakness

Severity: Unsuccessful Exploit

Background

Oracle Database is a relational database solution available for multiple platforms.

Problem

The Oracle Database service has accounts with default or easily guessed passwords, which could allow an attacker to make unauthorized SQL queries.

Resolution

Set a strong password for all database accounts.

References

http://www.dba-oracle.com/t_passwords_locking_changing_expiring.htm

Limitations

If successful, this exploit returns an SQL command shell, not an operating system command shell.

Oracle password weakness

Severity: Unsuccessful Exploit

Background

Oracle Database is a relational database solution available for multiple platforms.

Problem

The Oracle Database service has accounts with default or easily guessed passwords, which could allow an attacker to make unauthorized SQL queries.

Resolution

Set a strong password for all database accounts.

References

http://www.dba-oracle.com/t_passwords_locking_changing_expiring.htm

Limitations

If successful, this exploit returns an SQL command shell, not an operating system command shell.

Oracle MD2 component SDO_CODE_SIZE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1774

Background

Oracle Database is a relational database solution available for multiple platforms.

Problem

A buffer overflow in the SDO_CODE_SIZE function in the MD2 component of Oracle Database allows remote attackers to execute arbitrary commands.

Resolution

Apply the update referenced in Oracle Alert #68.

References

http://www.kb.cert.org/vuls/id/316206
http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0041.html

Limitations

Exploit works on Oracle Database 10g 10.1.0.2 and requires the login and password of a valid database user.

Oracle MD2 component SDO_CODE_SIZE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1774

Background

Oracle Database is a relational database solution available for multiple platforms.

Problem

A buffer overflow in the SDO_CODE_SIZE function in the MD2 component of Oracle Database allows remote attackers to execute arbitrary commands.

Resolution

Apply the update referenced in Oracle Alert #68.

References

http://www.kb.cert.org/vuls/id/316206
http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0041.html

Limitations

Exploit works on Oracle Database 10g 10.1.0.2 and requires the login and password of a valid database user.

Oracle Database OLAP component ODCITABLESTART buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-3974

Background

The Online Analytical Processing (OLAP) component of Oracle Database is a set of stored procedures used for multi-dimensional analytical queries.

Problem

A buffer overflow vulnerability in the ODCITABLESTART function allows command execution using a specially crafted SQL query.

Resolution

Apply the Oracle Critical Patch Update for January 2009.

References

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html

Limitations

Exploit works on Oracle Database 9i 9.0.2.1.

This exploit requires the login and password of a database account with EXECUTION privilege on the SYS.OLAPIMPL_T package. The default "scott" user has sufficient privilege.

Oracle Database OLAP component ODCITABLESTART buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-3974

Background

The Online Analytical Processing (OLAP) component of Oracle Database is a set of stored procedures used for multi-dimensional analytical queries.

Problem

A buffer overflow vulnerability in the ODCITABLESTART function allows command execution using a specially crafted SQL query.

Resolution

Apply the Oracle Critical Patch Update for January 2009.

References

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html

Limitations

Exploit works on Oracle Database 9i 9.0.2.1.

This exploit requires the login and password of a database account with EXECUTION privilege on the SYS.OLAPIMPL_T package. The default "scott" user has sufficient privilege.

Oracle Spatial component SDO_CS.TRANSFORM_LAYER buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5344

Background

The Oracle Spatial (formerly SDO) component of Oracle Database provides a set of functions which process multi-dimensional data.

Problem

A buffer overflow in the Oracle Spatial component allows an attacker with EXECUTE privileges on the SDO_CS.TRANSFORM_LAYER function to execute arbitrary commands.

Resolution

Apply the patch referenced in the October 2006 Oracle Critical Patch Update.

References

http://www.us-cert.gov/cas/techalerts/TA06-291A.html
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Limitations

Exploit works on Oracle Database 10.1.0.2 and 9.2.0.1.

Exploit requires a the login and password of a database user with privileges to create functions. The default "scott" user has sufficient privileges, but is disabled by default in Oracle Database 10g.

Oracle Spatial component SDO_CS.TRANSFORM_LAYER buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5344

Background

The Oracle Spatial (formerly SDO) component of Oracle Database provides a set of functions which process multi-dimensional data.

Problem

A buffer overflow in the Oracle Spatial component allows an attacker with EXECUTE privileges on the SDO_CS.TRANSFORM_LAYER function to execute arbitrary commands.

Resolution

Apply the patch referenced in the October 2006 Oracle Critical Patch Update.

References

http://www.us-cert.gov/cas/techalerts/TA06-291A.html
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Limitations

Exploit works on Oracle Database 10.1.0.2 and 9.2.0.1.

Exploit requires a the login and password of a database user with privileges to create functions. The default "scott" user has sufficient privileges, but is disabled by default in Oracle Database 10g.

Oracle Database string conversion buffer overflow

Severity: Unsuccessful Exploit

Background

Oracle Database is a relational database product for multiple platforms.

Problem

The string conversion function in Oracle Database is affected by a buffer overflow vulnerability. A remote attacker could execute arbitrary commands by sending a long argument to the **`to_char`** function with the **`systimestamp`** option.

Resolution

Apply the patch referenced in Oracle Alert 68.

References

http://www.us-cert.gov/cas/techalerts/TA04-245A.html
http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0041.html

Limitations

Exploit works on Oracle9i Database 9.2.0.1.

Exploit requires a valid database login and password.

Oracle Database string conversion buffer overflow

Severity: Unsuccessful Exploit

Background

Oracle Database is a relational database product for multiple platforms.

Problem

The string conversion function in Oracle Database is affected by a buffer overflow vulnerability. A remote attacker could execute arbitrary commands by sending a long argument to the **`to_char`** function with the **`systimestamp`** option.

Resolution

Apply the patch referenced in Oracle Alert 68.

References

http://www.us-cert.gov/cas/techalerts/TA04-245A.html
http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0041.html

Limitations

Exploit works on Oracle9i Database 9.2.0.1.

Exploit requires a valid database login and password.

Oracle Warehouse Builder SQL Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0799

Background

Oracle Warehouse Builder (OWB) is an ETL tool produced by Oracle that offers a graphical environment to build, manage and maintain data integration processes in business intelligence systems.

Problem

A SQL injection vulnerability exists in Oracle Warehouse Builder versions 10.2.0.5, 11.1.0.7, 11.2.0.1 and prior. An authenticated user with the *CONNECT* privilege may leverage this vulnerability to remotely compromise the server.

Resolution

Apply the April 2011 Oracle Critical Patch Update.

References

http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Limitations

This exploit has been tested against Oracle Business Intelligence Standard Edition One 10.1.3.2.1 on Windows Server 2003 SP2 (DEP OptOut). The exploit requires the login and password to an Oracle account with *connect* privileges. This exploit must bind to TCP port 80, so it needs root privileges to execute and no other process can be binding to port 80.

Oracle 9i Release 2 XDB HTTP Pass Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0727

##

Background

Oracle 9i release 2 includes the XDB HTTP service which by default listens on port 8080.

Problem

A buffer overflow vulnerability in the parsing of credentials passed to the server allows remote attackers to execute arbitrary commands by sending a long username or password during HTTP Basic authentication.

Resolution

The vulnerability is fixed in Oracle 9i version 9.2.0.4. To download and install the relevant patches follow the guide included in http://www.oracle.com/technology/deploy/security/pdf/2003Alert58.pdf.

References

http://otn.oracle.com/deploy/security/pdf/2003Alert58.pdf
http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-litchfield-paper.pdf
http://www.appsecinc.com/resources/alerts/oracle/2003-0005.html

Limitations

Exploit works against version 9.2.0.1

Oracle XDB component PITRIG_DROPMETADATA buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-4517

Background

The PITRIG_DROPMETADATA function is included in the XDB.XDB_PITRIG_PKG package which is included with Oracle Database.

Problem

A buffer overflow vulnerability in the PITRIG_DROPMETADATA function allows remote, authenticated attackers to execute arbitrary commands by specifying an OWNER and NAME parameter with a long combined length.

Resolution

This vulnerability will be fixed in a future Critical Patch Update from Oracle.

References

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=622

Limitations

Exploit works on Oracle Database 10g Release 2.

Exploit requires the login and password of a database user who has EXECUTE permission on package XDB.XDB_PITRIG_PKG. The default user "scott" has sufficient privilege if that account is enabled.

Oracle XDB component PITRIG_DROPMETADATA buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-4517

Background

The PITRIG_DROPMETADATA function is included in the XDB.XDB_PITRIG_PKG package which is included with Oracle Database.

Problem

A buffer overflow vulnerability in the PITRIG_DROPMETADATA function allows remote, authenticated attackers to execute arbitrary commands by specifying an OWNER and NAME parameter with a long combined length.

Resolution

This vulnerability will be fixed in a future Critical Patch Update from Oracle.

References

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=622

Limitations

Exploit works on Oracle Database 10g Release 2.

Exploit requires the login and password of a database user who has EXECUTE permission on package XDB.XDB_PITRIG_PKG. The default user "scott" has sufficient privilege if that account is enabled.

Oracle XDB component PITRIG_TRUNCATE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0339

Background

The PITRIG_TRUNCATE function is included in the XDB.XDB_PITRIG_PKG package which is included with Oracle Database.

Problem

A buffer overflow vulnerability in the PITRIG_TRUNCATE function allows remote, authenticated attackers to execute arbitrary commands by specifying an OWNER and NAME parameter with a long combined length.

Resolution

Apply the appropriate update referenced in the January 2008 Critical Patch Update.

References

http://www.us-cert.gov/cas/techalerts/TA08-017A.html

Limitations

Exploit works on Oracle Database Server 10g 10.1.0.5 and requires the login and password of an Oracle user with EXECUTE privileges on the XDB.XDB_PITRIG_PKG package.

Oracle XDB component PITRIG_TRUNCATE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0339

Background

The PITRIG_TRUNCATE function is included in the XDB.XDB_PITRIG_PKG package which is included with Oracle Database.

Problem

A buffer overflow vulnerability in the PITRIG_TRUNCATE function allows remote, authenticated attackers to execute arbitrary commands by specifying an OWNER and NAME parameter with a long combined length.

Resolution

Apply the appropriate update referenced in the January 2008 Critical Patch Update.

References

http://www.us-cert.gov/cas/techalerts/TA08-017A.html

Limitations

Exploit works on Oracle Database Server 10g 10.1.0.5 and requires the login and password of an Oracle user with EXECUTE privileges on the XDB.XDB_PITRIG_PKG package.

Oracle XML Component DBMS_XMLSCHEMA.GENERATESCHEMA buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-0272

Background

Oracle Database Server includes the **DBMS_XMLSCHEMA** component, which contains procedures for managing XML schemas.

Problem

A buffer overflow vulnerability in the **DBMS_XMLSCHEMA.GENERATESCHEMA** procedure allows database users to execute arbitrary commands.

Resolution

Install the patch referenced in the January 2006 Critical Patch Update.

References

http://www.kb.cert.org/vuls/id/545804
http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0037.html

Limitations

Exploit works on Oracle Database 10.1.0.2 and 9.2.0.1 and requires the login and password to an Oracle account with *connect* privileges.

Oracle XML Component DBMS_XMLSCHEMA.GENERATESCHEMA buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-0272

Background

Oracle Database Server includes the **DBMS_XMLSCHEMA** component, which contains procedures for managing XML schemas.

Problem

A buffer overflow vulnerability in the **DBMS_XMLSCHEMA.GENERATESCHEMA** procedure allows database users to execute arbitrary commands.

Resolution

Install the patch referenced in the January 2006 Critical Patch Update.

References

http://www.kb.cert.org/vuls/id/545804
http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0037.html

Limitations

Exploit works on Oracle Database 10.1.0.2 and 9.2.0.1 and requires the login and password to an Oracle account with *connect* privileges.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Windows password weakness

Severity: Unsuccessful Exploit **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

SQL injection authentication bypass

Severity: Unsuccessful Exploit

Background

Structured Query Language (SQL) is the most common language understood by modern relational databases.

Problem

A web program uses input parameters within an SQL query in an unsafe manner. This could allow a remote attacker to manipulate the authentication query via a specially crafted input parameter containing unexpected characters. A successful SQL injection attack could result in unauthorized access to the web application.

Resolution

Modify the web program to remove invalid characters from input parameters before using them in SQL queries.

References

http://www.windowsecurity.com/whitepapers/What-SQL-Injection.html

Limitations

In order for the exploit to succeed, the login form must be accessible by following links from the home page of a web site. The web program must allow authentication based on the response of a simple username and password query.

If using the https protocol, the exploit requires the IO-Socket-SSL PERL module to be installed on the scanning host. This module is available from http://www.cpan.org/modules/by-module/IO/.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

TFTP Server error packet buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2161

Background

TFTP Server is an open source server implementation of the tftp protocol for multiple platforms.

Problem

A buffer overflow vulnerability in the handling of error packets allows remote attackers to execute arbitrary commands.

Resolution

Upgrade to version 1.6 or higher when available, if that version contains a fix. Otherwise restrict access to the tftp service.

References

http://www.milw0rm.com/exploits/5563

Limitations

Exploit works on TFTP Server SP 1.4.

A different payload is required depending upon whether the service runs as a network service or standalone. Choose the first platform if TFTP Server is running as a network service, and the second if it is running standalone.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Trend Micro OfficeScan CGI programs POST request buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-3862

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending specially crafted HTTP POST requests to various CGI programs included in Trend Micro OfficeScan.

Resolution

Apply one of the patches referenced in Secunia advisory 32005.

References

http://secunia.com/secunia_research/2008-40/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch5 on Windows 2000 SP4, Windows Server 2003 SP2 without DEP, and Windows Server 2003 SP2 with patch KB933729 with DEP.

Trend Micro OfficeScan CGI programs POST request buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-3862

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending specially crafted HTTP POST requests to various CGI programs included in Trend Micro OfficeScan.

Resolution

Apply one of the patches referenced in Secunia advisory 32005.

References

http://secunia.com/secunia_research/2008-40/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch5 on Windows 2000 SP4, Windows Server 2003 SP2 without DEP, and Windows Server 2003 SP2 with patch KB933729 with DEP.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **`pwd`** parameter to the **`cgiABLogon.exe`** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **`pwd`** parameter to the **`cgiABLogon.exe`** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by

unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Windows DNS server RPC management interface buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-1748

Background

The Windows DNS service runs an RPC management interface which listens on a dynamically assigned TCP port.

Problem

A buffer overflow vulnerability in the Windows DNS service allows remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the management interface port.

Resolution

See Microsoft Security Advisory 935964 for information on available updates and workarounds.

References

http://www.us-cert.gov/cas/techalerts/TA07-103A.html

Limitations

Exploit works on Windows 2000 SP0 to SP4 and Windows Server 2003 SP1 and SP2.

Windows RPC DCOM interface buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0352

Background

The Distributed Component Object Model is a technology in Microsoft Windows operating systems which allows software components to communicate. Remote Procedure Call (RPC) is a protocol used to request a service from a program on another computer.

Problem

Insufficient input validation in the Windows RPCSS service leads to a buffer overflow in the DCOM process, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 03-026.

References

http://www.cert.org/advisories/CA-2003-16.html

Limitations

This exploit may cause the target system to crash.

Windows Server Service buffer overflow MS08-067

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4250

Background

The Windows Server service supports file, print, and named-pipe sharing over the network.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Windows Server service.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 08-067.

References

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

Limitations

Due to the nature of this vulnerability, the success of the exploit depends on the contents of unused stack memory space, and therefore is not completely reliable.

Windows Workstation service NetpManageIPCConnect buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4691

Background

The Windows Workstation service routes network requests for file or printer resources.

Problem

A buffer overflow in the NetpManageIPCConnect function in the Windows Workstation service allows command execution when a domain join request causes communication with a malicious domain controller.

Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new

mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

DNS

Severity: Service

SMB

Severity: Service

WWW (non-standard port 8000)

Severity: Service

WWW (non-standard port 8080)

Severity: Service

XDM (X login)

Severity: Service

blackjack (1025/TCP)

Severity: Service

epmap (135/TCP)

Severity: Service

h323gatedisc (1718/UDP)

Severity: Service

h323gatestat (1719/UDP)

Severity: Service

isakmp (500/UDP)

Severity: Service

jstel (1064/UDP)

Severity: Service

l2f (1701/UDP)

Severity: Service

microsoft-ds (445/TCP)

Severity: Service

microsoft-ds (445/UDP)

Severity: Service

ms-wbt-server (3389/TCP)

Severity: Service

ncube-lm (1521/TCP)

Severity: Service

netbios-dgm (138/UDP)

Severity: Service

netbios-ns (137/UDP)

Severity: Service

ntp (123/UDP)

Severity: Service

optima-vnet (1051/TCP)

Severity: Service

pptp (1723/TCP)

Severity: Service

tftp (69/UDP)

Severity: Service

4.6 10.8.0.104

IP Address: 10.8.0.104
Host type: Windows XP SP3
Scan time: Dec 14 12:50:21 2015
Netbios Name: XPSP3PATCHED

Windows password weakness (testadmin:testadmin)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Apache mod_rewrite LDAP URL buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3747

Background

mod_rewrite is an Apache module which allows rule-based modification of URL requests.

Problem

An off-by-one buffer overflow vulnerability in mod_rewrite allows command execution when the **`escape_absolute_uri`** function attempts to separate tokens within an LDAP URL.

Resolution

Upgrade to Apache HTTP Server version 1.3.37, 2.0.59, or 2.2.3 or higher.

References

http://archives.neohapsis.com/archives/bugtraq/2006-07/0514.html
http://www.kb.cert.org/vuls/id/395412

Limitations

Exploit works on Apache HTTP Server 2.0.58. The vulnerability is only exploitable when there exists a rule where the user can control the initial part of the rewritten URL. The rule must not contain a forbidden or gone flag [F or G] or the "noescape" [NE] flag.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

AWStats configdir parameter command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2005-0116

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

Insufficient validation of the **`configdir`** parameter before being used in a PERL open call leads to remote command execution.

Resolution

Upgrade to AWStats 6.3 or higher.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=185&type=vulnerabilities

Limitations

Exploit works on AWStats 6.2 on Linux.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **`base_qry_common.php`** script can be used to include arbitrary files under the directory specified by the **`BASE_path`** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **`base_qry_common.php`** script can be used to include arbitrary files under the directory specified by the **`BASE_path`** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with

the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://`*`target`*`/level/`*`xx`*`/exec/`*`command`***, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CMailServer CMailCOM.dll MoveToFolder buffer overflow

Severity: Unsuccessful Exploit

Background

CMailServer is a mail and web mail server.

The CMailServer web interface includes the **`CMailCOM.dll`** component which provides several classes.

Problem

A buffer overflow vulnerability in the **`MoveToFolder`** method of the POP3 class in **`CMailCOM.dll`** allows a remote attacker to execute arbitrary commands by requesting the **`mvmail.asp`** script with specially crafted arguments.

Resolution

Upgrade to version 5.4.7, which will presumably contain a fix, or higher when available.

References

http://secunia.com/advisories/30940/

Limitations

Exploit works on CMailServer 5.4.6.

In order for this exploit to succeed on Windows XP, the account used for anonymous access must be the IIS guest account (IWAM_XXX).

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

GitList blame resource command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4511

Background

GitList is a web-based git repository viewer.

Problem

A vulnerability in GitList allows remote attackers to execute arbitrary commands by sending a specially crafted request for the **`blame`** resource.

Resolution

Upgrade to GitList 0.5.0 or higher.

References

http://hatriot.github.io/blog/2014/06/29/gitlist-rce/

Limitations

The URL path to a gitlist repository must be known.

Hastymail rs parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4542

Background

Hastymail is a fast, secure, rfc-compliant, cross-platform IMAP/SMTP client application written in PHP providing a clean web interface for sending and reading E-mail.

Problem

Hastymail2 fails to properly sanitize user-supplied input passed to rs and rsargs[] parameters to the default URI. This can be exploited to execute arbitrary commands.

Resolution

Upgrade to Hastymail2 2.1.1-RC2 or later.

References

https://www.dognaedis.com/vulns/DGS-SEC-3.html

Limitations

This exploit has been tested against Hastymail2 2.1.0 on Windows XP SP3 and Hastymail2 2.1.1-RC1 on Ubuntu 10.04 Linux.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated,

the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IIS Double Decoding Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0333

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by URL-encoding invalid characters twice. Thus, a backslash is first represented as %5c, and then %255c. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 01-026.

References

http://archives.neohapsis.com/archives/bugtraq/2001-05/0101.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

IIS Unicode Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0884

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by encoding invalid characters in

Unicode. For example, a slash character is represented as %c0%af. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 00-078.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0263.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

Kolibri WebServer HTTP GET Request Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4158

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP GET requests. A remote attacker that supplies an overly long URI in a GET request could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-4158.html

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2, Windows 2003 SP2 and Windows 7 SP1.

Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-5289

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP POST requests. A successful remote attacker could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.securityfocus.com/archive/1/533150/30/270/threaded

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2 32-bit, Windows XP SP3 32-bit and Windows 7 32-bit and 64-bit.

Kolibri WebServer HTTP POST Request Handling Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-5289

Background

SENKAS Kolibri Webserver is a free very simple web server for Microsoft Windows that supports serving static web content.

Problem

Kolibri Webserver is vulnerable to a stack buffer overflow as a result of failure to properly validate user-supplied input when handling HTTP POST requests. A successful remote attacker could potentially execute arbitray code in the context of the Kolibri server.

Resolution

Deploy an alternate web server product or apply a patch when and if it becomes available.

References

http://www.securityfocus.com/archive/1/533150/30/270/threaded

Limitations

Exploit works against Kolibri Webserver 2.0 running on English versions of Windows XP SP2 32-bit, Windows XP SP3 32-bit and Windows 7 32-bit and 64-bit.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

MySQL password weakness

Severity: Unsuccessful Exploit

Background

MySQL is an open-source database software package available for multiple platforms.

Problem

A MySQL database account has no password or an easily guessed password, allowing a remote attacker to make unauthorized queries.

Resolution

Set a strong password for all MySQL accounts.

References

http://dev.mysql.com/doc/refman/5.0/en/default-privileges.html
http://dev.mysql.com/doc/refman/5.0/en/user-names.html

Limitations

The mysql client program is required.

If successful, this exploit returns an SQL command shell, not an operating system command shell.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2009-1350

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

A vulnerability in the **xtagent.exe** program allows remote, authenticated attackers to execute arbitrary commands by sending a specially crafted RPC message to the XTIERRPCPIPE named pipe which dereferences an arbitrary pointer.

Resolution

Apply the Novell NetIdentity 1.2.4 patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

Limitations

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

Novell Client nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5854

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **nwspool.dll** library in Novell Client is affected by buffer overflows in the **EnumPrinters** and **OpenPrinter** functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Apply **491psp3_nwspool.exe**. Patches are available from Novell.

References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***`%windir%`*`\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<`*`computername`*`>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<*computername*>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<*computername*>** for the exploit to work properly. Note that

users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **`%windir%\system32\cmd.exe`** must be granted to the Internet Guest Account **`IUSR_<computername>`** for the exploit to work properly. Note that users in the **`Users`** and **`Power Users`** groups do not have such privileges, but users in the **`Administrators`** and **`TelnetClients`** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **Toolbar.exe** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **Toolbar.exe** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **Toolbar.exe** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **Toolbar.exe** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception

management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP Remote File Inclusion

Severity: Unsuccessful Exploit

Background

PHP scripts support the **`include`** and **`require`** statements, which cause an outside script to be run within the calling script. The included script can be a local file or, in some configurations, the URL of a remote file.

Problem

The PHP script is vulnerable to a remote file inclusion vulnerability. This vulnerability typically arises due to an **`include`** or **`require`** command where the included file path can be manipulated by a remote user via a specific HTTP input parameter. A remote attacker could execute arbitrary PHP commands on the target by specifying the URL of a PHP script on his or her own server in the input parameter.

Resolution

Fix the vulnerable code so that included path names cannot be manipulated by the user.

The vulnerability can also be mitigated by setting the following variables in the PHP configuration file:

```
register_globals = Off
allow_url_include = Off
safe_mode = On
```

References

http://projects.webappsec.org/Remote-File-Inclusion

Limitations

This exploit works against Unix and Linux operating systems.

The exploit requires the **`register_globals`** and **`allow_url_include`** PHP settings to be on, and the **`safe_mode`** PHP setting to be off.

The **`telnet`** and **`mkfifo`** programs must exist on the target in order for the shell connection to be established.

phpBB viewtopic.php highlight parameter vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2086

Background

phpBB is an open-source bulletin board package written in PHP.

Problem

This is a variant of an older vulnerability which allows remote command execution by requesting **`viewtopic.php`** with a specially crafted **`highlight`** parameter.

Resolution

Upgrade to the latest version of phpBB.

References

http://archives.neohapsis.com/archives/bugtraq/2005-06/0256.html

phpRPC decode function command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2006-1032

Background

phpRPC is an xmlrpc library written in PHP supporting most databases.

Problem

A vulnerability in the **decode** function allows a remote attacker to execute arbitrary PHP commands placed inside a **<base64>** tag.

Resolution

phpRPC is no longer maintained by the author, so no fix is available. If phpRPC is installed as part of another product, contact the vendor of that product for a fix. Otherwise, remove phpRPC from the server.

References

http://archives.neohapsis.com/archives/bugtraq/2006-02/0507.html

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

RSA Authentication Agent for Web for IIS chunked encoding overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1471

Background

RSA Authentication Agent For Web for IIS provides access control for applications on IIS web servers.

Problem

A heap overflow vulnerability when using chunked transfer-encoding allows remote attackers to execute arbitrary commands with LocalSystem privileges.

Resolution

A fix is available from https://knowledge.rsasecurity.com.

References

http://www.kb.cert.org/vuls/id/790533
http://archives.neohapsis.com/archives/vulnwatch/2005-q2/0039.html

Limitations

Exploit works on RSA Authentication Agent For Web for IIS 5.3 on Windows 2000 SP4.

The success of this exploit depends on the system state at the time the exploit is attempted.

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English

(DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to

manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for

creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded

database on Windows Server 2003.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

TFTP Server error packet buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2161

Background

TFTP Server is an open source server implementation of the tftp protocol for multiple platforms.

Problem

A buffer overflow vulnerability in the handling of error packets allows remote attackers to execute arbitrary commands.

Resolution

Upgrade to version 1.6 or higher when available, if that version contains a fix. Otherwise restrict access to the tftp service.

References

http://www.milw0rm.com/exploits/5563

Limitations

Exploit works on TFTP Server SP 1.4.

A different payload is required depending upon whether the service runs as a network service or standalone. Choose the first platform if TFTP Server is running as a network service, and the second if it is running standalone.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Traq authenticate function remote code execution

Severity: Unsuccessful Exploit

Background

Traq is a PHP5+ and MySQL4+ based Project Tracking system with the ability to host multiple projects.

Problem

The flaw is caused due to admin rights not properly being restricted in the "authenticate()" function in admincp/common.php. This can be exploited to execute arbitrary code.

Resolution

Upgrade to Traq 2.3.1 or later.

References

http://www.exploit-db.com/exploits/18213
http://secunia.com/advisories/47108

Limitations

This exploit has been tested against Traq 2.3 on Linux.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **`pwd`** parameter to the **`cgiABLogon.exe`** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4008

Background

Oracle WebLogic Server (formerly BEA WebLogic Server) is a Java web application platform.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted Transfer-Encoding header in an HTTP request.

Resolution

Install the latest WebLogic Server plug-in referenced in the Oracle Security Advisory.

References

https://support.bea.com/application_content/product_portlets/securityadvisories/2806.html

Limitations

Exploit works on the WebLogic Server Connector for Apache 1.0.1136334.

WhatsUp Gold _maincfgret.cgi instancename buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0798

Background

WhatsUp Professional (formerly WhatsUp Gold) is a network mapping and monitoring tool.

Problem

A buffer overflow in the WhatsUp Gold web interface allows remote command execution by requesting **`_maincfgret.cgi`** with a long **`instancename`** parameter.

Resolution

Install WhatsUp Gold 8.03 Hotfix 1.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=133&type=vulnerabilities

Limitations

Exploit works on Ipswitch WhatsUp Gold 8.03.

Successful exploitation requires valid user credentials with permissions to *Configure Program* and *Configure Reports*.

Note that the WhatsUp Gold installation path may affect the success of this exploit. The exploit is designed to work with the default installation path only.

Windows LSASS buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0533

Background

The Local Security Authority Subsystem Service (LSASS) provides an interface for managing local security, domain authentication, and Active Directory processes.

Problem

A buffer overflow in the **`DsRolepInitializeLog`** function in the Windows LSASS service allows remote command execution.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 04-011.

References

http://www.kb.cert.org/vuls/id/753212

Limitations

This exploit may cause the target system to crash.

Windows Plug and Play buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1983

Background

The Windows Plug and Play service allows Windows operating systems to automatically detect and configure a new hardware device, such as a mouse.

Problem

A buffer overflow in the Plug and Play service could allow command execution with administrative privileges.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 05-047.

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Limitations

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

Windows RPC DCOM interface buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0352

Background

The Distributed Component Object Model is a technology in Microsoft Windows operating systems which allows

software components to communicate. Remote Procedure Call (RPC) is a protocol used to request a service from a program on another computer.

Problem

Insufficient input validation in the Windows RPCSS service leads to a buffer overflow in the DCOM process, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 03-026.

References

http://www.cert.org/advisories/CA-2003-16.html

Limitations

This exploit may cause the target system to crash.

Windows RRAS memory corruption vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2370

Background

The Routing and Remote Access Service (RRAS) allows a Windows computer to act as a router, dial-up access server, VPN server, or network address translator.

Problem

A buffer overflow in RRAS allows remote attackers to execute arbitrary commands.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 06-025.

References

http://www.kb.cert.org/vuls/id/631516

Limitations

The Remote Access Connection Manager service must be running in order for this exploit to succeed.

On Windows 2000, the Routing and Remote Access service must also be running and configured, and valid Windows login credentials are required. (Credentials are not required on Windows XP.)

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows 2000. These packages are available from http://cpan.org/modules/by-module/.

Windows Server Service buffer overflow MS08-067

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4250

Background

The Windows Server service supports file, print, and named-pipe sharing over the network.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Windows Server service.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 08-067.

References

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

Limitations

Due to the nature of this vulnerability, the success of the exploit depends on the contents of unused stack memory space, and therefore is not completely reliable.

Wireshark DECT Dissector Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-1591

Background

Wireshark is a network packet analyzer.

Problem

A buffer overflow vulnerability in the DECT dissector allows command execution when a user sends a specially crafted datagram over a network which is being analyzed by Wireshark.

Resolution

Upgrade to Wireshark 1.4.5 or higher.

References

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Limitations

Exploit works on Wireshark 1.4.4.

The affected target running Wireshark must be on the same network as as the SAINTexploit host.

Exploit requires the Net-Write PERL module to be installed on the scanning host. This module is available from http://search.cpan.org/dist/Net-Write/lib/Net/Write.pm.

The "Wireshark DECT Dissector PCAP File Processing Overflow" client exploit attempts to exploit the same

vulnerability. The client exploit does not have the same network and PERL module limitations, but requires user cooperation.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

Xi Software Net Transport eDonkey Protocol Buffer Overflow

Severity: Unsuccessful Exploit

Background

Net Transport, also known as NetXfer, is a download manager for Windows made by Xi Software. Among the protocols Net Transport can handle is eDonkey, a decentrailized peer to peer network for file sharing.

Problem

The Net Transport download manager fails to properly sanitize user input from the eDonkey network, specifically in processing eDonkey **`OP_LOGINREQUEST`** packets. A successful attacker sending a specially crafted packet could cause a stack buffer overflow and execute arbitrary code.

Resolution

Restrict access to the port used for eDonkey. Upgrade to a newer version of Net Transport that contains a fix.

References

http://secunia.com/advisories/38028/

Limitations

Exploit runs on Xi Software Net Transport 2.90.510.
The eDonkey service port must be known by the attacker. By default, the application uses a random port.
The exploit may take a longer time to establish a shell connection.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that

users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

DNS

Severity: Service

SMB

Severity: Service

WWW

Severity: Service

WWW (non-standard port 5985)

Severity: Service

XDM (X login)

Severity: Service

epmap (135/TCP)

Severity: Service

h323gatedisc (1718/UDP)

Severity: Service

h323gatestat (1719/UDP)

Severity: Service

isakmp (500/UDP)
Severity: Service

microsoft-ds (445/TCP)
Severity: Service

microsoft-ds (445/UDP)
Severity: Service

ms-wbt-server (3389/TCP)
Severity: Service

mysql (3306/TCP)
Severity: Service

netbios-dgm (138/UDP)
Severity: Service

netbios-ns (137/UDP)
Severity: Service

ntp (123/UDP)
Severity: Service

ssdp (1900/UDP)
Severity: Service

tftp (69/UDP)
Severity: Service

4.7 10.8.0.150

IP Address: 10.8.0.150
Scan time: Dec 14 12:46:20 2015
Host type: Windows Server 2008 R2
Netbios Name: WIN-IQF3U12CJA5

Windows password weakness (netbank:netbank)
Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (testadmin:testadmin)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

Windows password weakness (testuser:testuser)

Severity: Remote User **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability

with **openssl**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **MIME::Base64** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **exec()** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **openssl**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **MIME::Base64** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

Apache mod_rewrite LDAP URL buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3747

Background

mod_rewrite is an Apache module which allows rule-based modification of URL requests.

Problem

An off-by-one buffer overflow vulnerability in mod_rewrite allows command execution when the **`escape_absolute_uri`** function attempts to separate tokens within an LDAP URL.

Resolution

Upgrade to Apache HTTP Server version 1.3.37, 2.0.59, or 2.2.3 or higher.

References

http://archives.neohapsis.com/archives/bugtraq/2006-07/0514.html
http://www.kb.cert.org/vuls/id/395412

Limitations

Exploit works on Apache HTTP Server 2.0.58. The vulnerability is only exploitable when there exists a rule where the user can control the initial part of the rewritten URL. The rule must not contain a forbidden or gone flag [F or G] or the "noescape" [NE] flag.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

Avaya IP Office Customer Call Reporter ImageUpload.ashx file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3811

Background

Avaya IP Office is a unified communications solution for mobile workforce.

Problem

The ImageUpload.ashx script allows unauthenticated users to upload arbitrary script files to the webserver. The script files can then be executed by a web request, leading to arbitrary command execution.

Resolution

Apply one of the fixes referenced in ASA-2012-222.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-106/

Limitations

Exploit works on Avaya IP Office Customer Call Reporter 8.0.8.15.

AWStats configdir parameter command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2005-0116

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

Insufficient validation of the **`configdir`** parameter before being used in a PERL open call leads to remote command execution.

Resolution

Upgrade to AWStats 6.3 or higher.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=185&type=vulnerabilities

Limitations

Exploit works on AWStats 6.2 on Linux.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **migrate** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **AllowToUpdateStatsFromBrowser** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include

arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **base_qry_common.php** script can be used to include arbitrary files under the directory specified by the **BASE_path** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA ARCserve D2D Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

CA ARCserve D2D is a disk-based backup solution.

Problem

CA ARCserve D2D deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA Total Defense UNCWS exportReport SQL Injection

Severity: Unsuccessful Exploit

Background

CA Total Defense is a combined host-based anti-virus, anti-spyware, firewall, and IPS solution.

Problem

CA Total Defense includes a web service management component, which in version r12 prior to SE3, fails to validate certain parameters. The exportReport function of this service is vulnerable to a SQL Injection attack.

Resolution

Upgrade to CA Total Defense r12 SE3 (Build 831) or later.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-022/
http://secunia.com/advisories/47883/

Limitations

Tested against CA Total Defense Suite 12.0.528 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The target server must be configured to listen on the HTTP port.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

CA XOsoft Control Service entry_point.aspx Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1223

Background

CA XOsoft is storage and recovery management software that includes applications for combined business continuity and disaster recovery. The CA XOsoft product family includes CA XOsoft Replication, CA XOsoft High Availability, and CA XOsoft Content Distribution.

Problem

Control Service r12 and Control Service r12.5 included in the CA XOsoft Replication, High Availability, and Content Distribution products with versions r12 and r12.5 are vulnerable to a stack buffer overflow as a result of overly long data passed to **`/entry_point.aspx`**. A successful attacker could execute arbitrary code with the permissions of the CA Control Service process.

Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

References

http://secunia.com/advisories/39337/

Limitations

Exploit works on CA XOsoft Control Service r12.5.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://`*`target`*`/level/`*`xx`*`/exec/`*`command`***, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy Chat Server Authentication Request Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy Chat Server is a web-based chat server for Microsoft Windows.

Problem

The server is vulnerable to a remote buffer-overflow attack which can be triggered by sending a specially crafted **`password`** parameter to **`chat.ghp`**.

Resolution

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

References

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

Limitations

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Management Web Server UserID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit

Background

Easy File Management Web Server is a Microsoft Windows based file management application that allows remote users to upload and download files through a web browser. It also supports online editing of Word, Excel, PowerPoint and PDF documents on the server by a user with just a browser.

Problem

Easy File Management Web Server 4.0 and 5.3 are vulnerable to remote stack buffer overflow as a result of not properly validating user-supplied input when handling the **`UserID`** cookie. A successful remote attacker could execute arbitrary code with the privileges of the system user.

Resolution

Contact the vendor for information on when a fix will be available. In the interim, only allow trusted sites to access the application.

References

http://www.securelist.com/en/advisories/58879

Limitations

Exploit works on Easy File Management Web Server v4.0 and v5.3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html
http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

Easy File Sharing Web Server SESSIONID Cookie Handling Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2014-3791

Background

Easy File Sharing Web Server is software that allows users to upload/download files to a server easily through a web browser, as well as providing a bulletin board system (forum).

Problem

Easy File Sharing Web Server is vulnerable to a stack buffer overflow condition as a result of not properly validating user-supplied input when handling a SESSIONID cookie. This allows a remote attacker to potentially execute arbitrary code.

Resolution

Install a fixed version when one becomes available. Alternatively, find a different software product solution.

References

http://www.zerodaylab.com/vulnerabilities/CVE-2014/CVE-2014-3791.html

http://blog.techorganic.com/2014/05/14/from-fuzzing-to-0-day/

Limitations

Exploit works on Windows XP Professional SP2 and SP3.

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EMC AlphaStor Device Manager Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-0928

Background

EMC AlphaStor is a media lifecycle and tape library management product for enterprise environments.

Problem

EMC AlphaStor versions prior to 4.0 Build 800 are vulnerable to remote command injection. The AlphaStor Device Manager (`rrobotd.exe`) contains a flaw which could be exploited to inject arbitrary commands via the DCP run command.

Resolution

Upgrade to version 4.0 build 800 or later.

References

http://secunia.com/advisories/51930/

Limitations

This exploit was tested against EMC AlphaStor 4.0 build 114 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications

to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

EnterpriseDB PostgreSQL Plus Advanced Server DBA Management Server Authentication

Severity: Unsuccessful Exploit

Background

Postgres Plus Advanced Server is an enterprise database solution. It includes several productivity tools, such as Migration Studio, Postgres Studio, DBA Management Server, and DBA Monitoring Console.

Problem

An authentication bypass vulnerability exists in the browser-based DBA Management Server tool included with EnterpriseDB Postgres Plus Advanced Server versions 8.x prior to 8.4.7.20. Postgres Plus Advanced Server uses JBoss Application Server to execute the DBA Management Server. The JBoss configuration does not limit access to the jmx-console and web-console applications. Unauthenticated clients can use these applications to upload and execute malicious files.

Resolution

Update DBA Management Server to Build 39, or remove the jmx-console and web-console applications from the Postgres Plus Advanced Server.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-102/
http://secunia.com/advisories/43590/

Limitations

This exploit works against EnterpriseDB Postgres Plus Advanced Server 8.4.5.18 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

FrontPage fp30reg.dll remote debug buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0822

Background

Microsoft FrontPage Server Extensions includes a remote debugging function.

Problem

A buffer overflow in **`fp30reg.dll`** leads to a vulnerability in the remote debug function in FrontPage Server Extensions. A remote attacker could execute arbitrary commands using a specially crafted chunked encoded request.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 03-051.

References

http://www.kb.cert.org/vuls/id/279156

GitList blame resource command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2014-4511

Background

GitList is a web-based git repository viewer.

Problem

A vulnerability in GitList allows remote attackers to execute arbitrary commands by sending a specially crafted request for the **`blame`** resource.

Resolution

Upgrade to GitList 0.5.0 or higher.

References

http://hatriot.github.io/blog/2014/06/29/gitlist-rce/

Limitations

The URL path to a gitlist repository must be known.

Hastymail rs parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4542

Background

Hastymail is a fast, secure, rfc-compliant, cross-platform IMAP/SMTP client application written in PHP providing a clean web interface for sending and reading E-mail.

Problem

Hastymail2 fails to properly sanitize user-supplied input passed to rs and rsargs[] parameters to the default URI. This can be exploited to execute arbitrary commands.

Resolution

Upgrade to Hastymail2 2.1.1-RC2 or later.

References

https://www.dognaedis.com/vulns/DGS-SEC-3.html

Limitations

This exploit has been tested against Hastymail2 2.1.0 on Windows XP SP3 and Hastymail2 2.1.1-RC1 on Ubuntu 10.04 Linux.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP Intelligent Management Center mibFileUpload Servlet Unrestricted File Creation

Severity: Unsuccessful Exploit **CVE:** CVE-2012-5201

Background

HP Intelligent Management Center (IMC), also known as HP iNode Management Center, is a comprehensive management platform for delivering integrated, modular network management capabilities.

Problem

HP IMC 5.1 E0202 and earlier is vulnerable to remote code execution as a result of the **`mibFileUpload`** servlet allowing an unauthenticated remote attacker to create arbitrary files on the vulnerable server. A successful attacker could execute arbitrary code on the server in the context of the SYSTEM user.

Resolution

Apply updates as directed in HP Security Bulletin HPSBGN02854 SSRT100881.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-050/

Limitations

This exploit was tested against HP Intelligent Management Center v5.1 E0202 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 with DEP OptOut.

The Perl module **`Archive::Zip`** is required to run the exploit.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP LoadRunner Virtual User Generator EmulationAdmin service directory traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4837

Background

HP LoadRunner is a software performance testing solution.

Problem

A directory traversal vulnerability in the Virtual User Generator EmulationAdmin service allows remote attackers to upload files to arbitrary locations using the copyFileToServer method. The files could then be executed via an HTTP request.

Resolution

Apply LoadRunnner patch v11.52.1, which can be downloaded from HP Software Support Online (SSO).

References

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03969437
http://www.zerodayinitiative.com/advisories/ZDI-13-259/

Limitations

Exploit works on HP LoadRunner 11.52. HP LoadRunner must be installed in the standard installation path.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **`coda.exe`** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x34 vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2019

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-114/

Limitations

Exploit works on HP Operations Agent 11.00.

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Agent Opcode 0x8c vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2020

Background

HP Operations Agents is a fault and performance monitoring solution for servers.

Problem

A buffer overflow vulnerability in the **coda.exe** process, which listens on a random TCP port, could allow remote attackers to execute arbitrary code by sending a specially crafted GET request.

Resolution

Apply the patch referenced in HPSBMU02796 SSRT100594.

References

http://www.zerodayinitiative.com/advisories/ZDI-12-115/

Limitations

This exploit has been tested against HP Operations Agent 11.00 on Windows Server 2003 SP2 English (DEP OptOut).

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP Operations Manager hidden Tomcat account

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3843

Background

HP Operations Manager is a consolidated event and performance management console that correlates infrastructure, network and end-user experience events across an IT infrastructure.

Problem

A hidden Apache Tomcat account allows remote attackers to use the org.apache.catalina.manager.HTMLManagerServlet class to upload arbitrary files, leading to arbitrary code execution.

Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2

English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP OpenView Performance Insight Server Backdoor Account

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0276

Background

HP OpenView Performance Insight (OVPI) Server is a management utility that monitors and reports on the performance of services.

Problem

A backdoor account may allow an attacker to execute arbitrary code on the system.

Resolution

Apply patch 5.41.002 piweb HF02.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Performance Manager Apache Tomcat Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3548

Background

HP Performance Manager Software is a web-based analysis and visualization tool that analyzes performance trends of applications, systems, and services. HP Performance Manager incorporates Apache Tomcat 5 to help serve custom web applications.

Problem

An unauthorized file upload vulnerability exists in HP Performance Manager. HP Performance Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

References

http://secunia.com/advisories/39847/

Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formExportDataLogs buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3999

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability HP Power Manager allows remote attackers to execute arbitrary commands by sending an HTTP POST request for the formExportDataLogs program with a specially crafted fileName parameter.

Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager formLogin buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4113

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A buffer overflow vulnerability in the Administration interface allows remote attackers to execute arbitrary commands by sending a request for the formLogin program with a specially crafted Login parameter.

Resolution

Upgrade to HP Power Manager 4.3.2.

References

http://www.securityfocus.com/archive/1/515283

Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to

execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP Power Manager Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2685

Background

HP Power Manager is a web-based application that enables administrators to manage an HP UPS from a browser-based management console.

Problem

A stack-based buffer overflow in the HP Power Manager management web server allows remote attackers to execute arbitrary code via the Login variable of the login form.

Resolution

HP's resolution is to limit access to trusted users.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope SOAP Call APIPreferenceImpl Security Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3261

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications

and application components.

Problem

HP SiteScope versions 11.10, 11.11, and 11.12 are vulnerable to remote code execution via a vulnerable SOAP call using **`APIPreferenceImpl`**.

Resolution

Upgrade to SiteScope v11.13 or newer. In addition, an administrator must disable the vulnerable SOAP API by adding the **`_disableOldAPIs=true`** property to the **`master.config`** file.

References

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03489683

Limitations

This exploit has been tested against HP SiteScope 11.20 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP SiteScope APIBSMIntegrationImpl runOMAgentCommand SOAP Request Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2367

Background

HP SiteScope is an agentless software application used to monitor the availability and performance of distributed IT infrastructures including servers, operating systems, network and Internet services, applications and application components.

Problem

HP SiteScope is vulnerable to remote code execution because the runOMAgentCommand in an APIBSMIntegrationImpl SOAP request does not properly sanitize user-supplied input. By supplying a windows shell command to the omHost key, an attacker can execute arbitrary commands with SYSTEM privileges.

Resolution

Upgrade to SiteScope v11.22 or higher.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-205/

Limitations

This exploit was tested against HP SiteScope 11.20 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

HP Universal CMDB Server Axis2 default password

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0219

Background

HP Universal CMDB Server 9.0 is a modular management system that consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

Problem

HP UCMDB deploys Axis2 with default credentials which can be used to gain unauthorized access to the web application server. By then uploading a specially crafted axis2 service, an attacker could execute arbitrary commands on the system.

Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

References

http://www.securityfocus.com/archive/1/515494

Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IBM Rational Quality Manager and Test Lab Manager Policy Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4094

Background

IBM Rational Quality Manager is a web-based centralized test management environment for test planning, workflow control, tracking and metrics reporting. IBM Rational Quality Manager incorporates Apache Tomcat 5 to help serve custom web applications.

IBM Rational Test Lab Manager integrates fully with Rational Quality Manager and helps to improve the efficiency of the test lab and optimize how resources are requested and provided.

Problem

An unauthorized file upload vulnerability exists in IBM Rational Quality Manager. IBM Rational Quality Manager generates credentials for a default user/password combination in Apache Tomcat. A remote attacker can leverage this vulnerability by sending a crafted HTTP request using the default credentials. Once authenticated, the attacker can upload a malicious web application to a vulnerable system.

Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

IIS Double Decoding Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0333

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by URL-encoding invalid characters twice. Thus, a backslash is first represented as %5c, and then %255c. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 01-026.

References

http://archives.neohapsis.com/archives/bugtraq/2001-05/0101.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

IIS Unicode Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0884

Background

Microsoft IIS is a web server for Windows platforms.

Problem

Microsoft IIS 4.0 and 5.0 allow path validation checks to be bypassed by encoding invalid characters in Unicode. For example, a slash character is represented as %c0%af. This allows remote attackers to access any executable file on the system using a directory traversal attack from the /scripts virtual directory, leading to command execution.

Resolution

Install the patch referenced in Microsoft Security Bulletin 00-078.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0263.html

Limitations

Certain characters are disallowed when using this exploit to run commands.

IMail LDAP buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0297

Background

IMail is an e-mail server for Windows platforms. It includes a service which implements the Lightweight Directory Access Protocol (LDAP).

Problem

A buffer overflow in IMail's LDAP service allows a remote attacker to overwrite the Global Exception Handler by sending long, specially crafted tags, leading to command execution.

Resolution

Upgrade to the latest version of IMail or apply IMail 8.05 Hotfix 2.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=74

Limitations

Exploit works on IMail 8.0.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

InterSystems Cache HTTP Stack Buffer Overflow

Severity: Unsuccessful Exploit

Background

InterSystems Cache is a high-performance object database that also enables rapid Web application development.

Problem

Intersystems Cache is vulnerable to a HTTP stack buffer overflow as a result of a specially crafted parameter to the UtilConfigHome.csp page.

Resolution

Upgrade or apply a patch when it becomes available.

References

None available at this time.

Limitations

None.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS

distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0738

Background

JBoss Application Server (AS) is a full-featured open source Java application server that includes full support for J2EE-based APIs. JBoss AS runs on numerous operating systems (e.g., Linux, FreeBSD, Mac OS X, and Microsoft Windows), as long as a suitable Java Virtual Machine (JVM) is present.

Java Management Extensions (JMX) is a Java technology that provides tools for managing and monitoring applications, system objects, devices (e.g., printers) and service oriented networks. JMX Console is a JMX-based management console application for JBoss AS that comes bundled with the JBoss AS distribution.

Problem

JMX Console uses HTTP password authentication to control access to the application. However, JBoss AS allows verb-based authentication and access control (VBAAC), which allows specifying different access controls for different HTTP verbs (e.g., GET, POST, HEAD). The default JBoss AS authentication configuration restricts access to JMX Console via HTTP GET and POST verbs to users in the JBossAdmin role, but

there is no restriction placed on access via other HTTP verbs. Since HEAD requests are executed by the GET verb handler, any command embedded in a HTTP HEAD request will be executed the same way as the same command using the GET request, but without requiring authentication and without sending the response body to the requester. By sending a crafted HTTP request with a verb other than GET or POST to the target server, a remote unauthenticated attacker can inject and execute arbitrary unrestricted Java code on the target server, including file access and invocation of command shell, in the context of the JBoss AS process, normally jboss on *NIX systems and SYSTEM on Windows systems.

Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

References

http://secunia.com/advisories/39563/

Limitations

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1195

Background

LANDesk Lenovo ThinkManagement Console provides hardware discovery, comprehensive inventory, and reporting for Lenovo systems.

Problem

LANDesk Lenovo ThinkManagement Console runs a web application under the Microsoft IIS web server. This web application exposes some web services that do not require authentication. In versions up to 9.0.3, the 'ServerSetup.asmx' web service, which is accessible without authentication, is vulnerable to a file upload vulnerability. This can be exploited by an attacker to upload a malicious server-side script to the server, then request it via the web interface, causing its contents to be executed on the server. This allows the attacker control execution on the server.

Resolution

No updates are available at this time. Limit network access to the LANDesk Lenovo ThinkManagement Console to hosts to administrators only.

References

http://secunia.com/advisories/47666
http://retrogod.altervista.org/9sg_landesk_adv.htm
http://community.landesk.com/support/docs/DOC-24787

Limitations

This exploit has been tested against LANDesk Lenovo ThinkManagement Suite 9.0.2 on Windows Server 2003 SP2 English (DEP OptOut). After successful exploitation, a file will be uploaded to /upl/exploit.asp on the server. When executed, a randomly named .EXE file will be created in the filesystem root. Both files should be manually removed after exploitation.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument

http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

Lotus Domino HPRAgentName Stack Overflow

Severity: Unsuccessful Exploit

Background

IBM Lotus Domino is a messaging and collaboration solution for multiple platforms.

Problem

The WebAdmin.nsf resource on the Domino web service contains a buffer overflow vulnerability.

Resolution

No patch is available at this time.

References

http://www-10.lotus.com/ldd/r5fixlist.nsf/Public/7BE022D035F58F8D8525786F007EC417?OpenDocument
http://www.research.reversingcode.com/index.php/advisories/73-ibm-ssd-1012211

Limitations

This exploit has been tested against IBM Lotus Domino 8.5 on Windows Server 2003 SP2 English (DEP AlwaysOff). This exploit requires valid credentials for an account that is able to access the /webadmin.nsf resource.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Firewall Reporter isValidClient Authentication Bypass

Severity: Unsuccessful Exploit

Background

McAfee Firewall Reporter is an enterprise-class security event management (SEM) reporting solution.

Problem

McAfee Firewall Reporter versions 5.1.0.6 through 5.1.0.12 are vulnerable to an authentication bypass that may allow remote attackers to upload files to the server. This may allow attackers to upload and execute

arbitrary code.

Resolution

Upgrade to McAfee Firewall Reporter version 5.1.0.13 or later.

References

https://kc.mcafee.com/corporate/index?page=content&id=SB10015
http://www.zerodayinitiative.com/advisories/ZDI-11-117/
http://secunia.com/advisories/44110/

Limitations

This exploit has been tested against McAfee Firewall Reporter 5.1.0.6 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).
The exploit creates two files on the server which persist after the shell connection is terminated: c:\exploit.exe and /cgi-bin/exploit.cgi. These files should be removed manually after successful exploitation.

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-4810

Background

McAfee Web Reporter analyzes logs from a variety of proxy sources to provide real-time views into web traffic, including extensive drill-down capabilities and powerful off-line processing.

Problem

McAfee Web Reporter is vulnerable to remote code execution due to embedding a vulnerable version of JBoss. The vulnerability is due to the application not properly restricting access to the invoker /EJBInvokerServlet which can be exploited to deploy and execute arbitray Java code by sending a specially crafted marshalled object to TCP port 9111.

Resolution

Contact the vendor for a solution.

References

http://secunia.com/advisories/55112/
http://retrogod.altervista.org/9sg_ejb.html

Limitations

This exploit was tested against McAfee Web Reporter 5.2.1 on Windows Server 2008 R2 SP1 (DEP OptOut).

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Windows NetDDE buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0206

Background

Network Dynamic Data Exchange (NetDDE) is a Windows service which allows two applications to communicate with each other over a network.

Problem

A buffer overflow in the NetDDE service could allow a remote, anonymous attacker to execute arbitrary commands by sending a specially crafted NetDDE message to the vulnerable system.

Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2009-1350

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

A vulnerability in the **`xtagent.exe`** program allows remote, authenticated attackers to execute arbitrary commands by sending a specially crafted RPC message to the XTIERRPCPIPE named pipe which dereferences an arbitrary pointer.

Resolution

Apply the Novell NetIdentity 1.2.4 patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

Limitations

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

Novell Client nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5854

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflows in the **`EnumPrinters`** and **`OpenPrinter`** functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Apply **`491psp3_nwspool.exe`**. Patches are available from Novell.

References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

Novell Client 4.91 SP4 nwspool.dll buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6701

Background

Novell Client software provides NetWare connectivity to Windows platforms.

Problem

The **`nwspool.dll`** library in Novell Client is affected by buffer overflow vulnerabilities in several different functions, allowing remote attackers to execute arbitrary commands by sending a specially crafted RPC request to the Spooler service.

Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager EnteredClassName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1929

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

A buffer overflow vulnerability in jclient.dll allows remote attackers to execute arbitrary commands by sending a specially crafted EnteredClassName parameter to the nps/servlet/webacc program.

Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

References

http://secunia.com/advisories/40281

Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

Novell iManager getMultiPartParameters file upload vulnerability

Severity: Unsuccessful Exploit

Background

Novell iManager is a web-based management interface for other Novell products.

Problem

The **`getMultiPartParameters`** function in the **`nps.jar`** web application in Novell iManager allows remote attackers to upload arbitrary files to the server. By uploading a script file to a web-accessible location on the server, this vulnerability can result in remote command execution.

Resolution

Apply the patch referenced in Novell document 7006515.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

Limitations

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname

parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1555

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted Hostname parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://zerodayinitiative.com/advisories/ZDI-10-086/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1554

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted ICount parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be

granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1553

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in Network Node Manager allows remote attackers to execute arbitrary commands by sending a request for the getnnmdata.exe CGI program with a specially crafted MaxAge parameter.

Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`jovgraph.exe`** allows remote attackers to execute arbitrary commands by sending an overly long **`displayWidth`** option in the **`arg`** parameter to the **`jovgraph.exe`** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **jovgraph.exe** allows remote attackers to execute arbitrary commands by sending an overly long **displayWidth** option in the **arg** parameter to the **jovgraph.exe** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **jovgraph.exe** allows remote attackers to execute arbitrary commands by sending an overly long **displayWidth** option in the **arg** parameter to the **jovgraph.exe** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0261

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **jovgraph.exe** allows remote attackers to execute arbitrary commands by sending an overly long **displayWidth** option in the **arg** parameter to the **jovgraph.exe** CGI program.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that

users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-3848

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **Template** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/advisories/37665/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0268

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a specially crafted **nameParams/text1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_<computername>** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that

users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-0269

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **nnmRptConfig.exe** CGI program with a long, specially crafted **schdParams/schd_select1** parameter.

Resolution

Apply the appropriate patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file ***%windir%*\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the **Users** and **Power Users** groups do not have such privileges, but users in the **Administrators** and **TelnetClients** groups do.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **OpenView5.exe** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager OpenView5.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in the **`OpenView5.exe`** CGI program allows remote attackers to execute arbitrary commands.

Resolution

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4179

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the **`ovalarm.exe`** CGI program allows command execution when an attacker sends an HTTP request to this program with a specially crafted Accept-Language header.

Resolution

See HPSBMA02483 SSRT090257 rev.2 for patch information.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

HP OpenView Network Node Manager OVBuildPath Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3167

Background

HP OpenView Network Node Manager (NNM) is a network monitoring solution based on SNMP.

Problem

User supplied data from the NNM web interface is passed to the OVBuildPath function in ov.dll. This function contains a stack overflow vulnerability that may allow an unauthenticated attacker to take control of the server.

Resolution

No patches are available at this time. Restrict access to the web interface of the NNM server.

References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03054052
http://www.zerodayinitiative.com/advisories/ZDI-12-002/
http://www.zerodayinitiative.com/advisories/ZDI-12-003/

Limitations

This exploit has been tested against HP OpenView Network Node Manager 7.53 on Windows Server 2003 SP2 English (DEP OptOut) with KB956802 and KB2393802.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovlogin.exe buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-6204

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow in the Network Node Manager web interface allows remote attackers to execute arbitrary commands by sending a long, specially crafted argument to the **`ovlogin.exe`** CGI program.

Resolution

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

Limitations

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **`ovwebsnmpsrv.exe`** allows remote attackers to execute arbitrary commands by sending specially crafted **`sel`** and **`arg`** parameters to the **`jovgraph.exe`** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **ovwebsnmpsrv.exe** allows remote attackers to execute arbitrary commands by sending specially crafted **sel** and **arg** parameters to the **jovgraph.exe** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

Severity: Unsuccessful Exploit **CVE:** CVE-2009-4181

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability in **ovwebsnmpsrv.exe** allows remote attackers to execute arbitrary commands by sending specially crafted **sel** and **arg** parameters to the **jovgraph.exe** CGI program.

Resolution

Apply the fix referenced in HPSBMA02483 SSRT090257.

References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-1552

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A stack buffer overflow vulnerability in HP Openview NNM allows remote attackers to execute arbitrary commands by sending specially crafted **act** and **app** parameters to the **snmpviewer.exe** CGI program.

Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

References

http://secunia.com/advisories/39757/

Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, **Read** and **Execute** privileges on the file **%windir%\system32\cmd.exe** must be granted to the Internet Guest Account **IUSR_*<computername>*** for the exploit to work properly. Note that users in the groups **Users** and **Power Users** don't have those privileges, but users in the groups **Administrators** and **TelnetClients** do.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-0067

Background

HP OpenView Network Node Manager is network availability and performance management software.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by requesting the **`Toolbar.exe`** CGI program with a long, specially crafted parameter.

Resolution

Apply a fix when available, or restrict access to the **`Toolbar.exe`** CGI program.

References

http://secunia.com/secunia_research/2008-13/

Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Business Transaction Management FlashTunnelService WriteToFile Vulnerability

Severity: Unsuccessful Exploit

Background

Oracle Business Transaction Management (BTM) is a component of several Oracle Enterprise Manager Management Packs, including WebLogic Server Management Pack Enterprise Edition. Oracle BTM provides capability in three key areas: transaction visibility, performance and SLA management, and exception management.

Problem

Oracle Business Transaction Management 12.1.0.2.7, as delivered with Oracle WebLogic Server 12c (12.1.1), is vulnerable to remote code excecution as a result of a directory traversal vulnerability. Oracle BTM server installs a web service called **`FlashTunnelService`** which processes incoming SOAP requests without requiring prior authentication. This SOAP interface exposes the **`writeToFile`** function which could allow a remote attacker to write arbitrary files on the target server by exploiting a directory traversal vulnerability associated with the "handle" property to control the file location. By using the "text" element to control the file contents, an attacker can create an arbitrary JavaServer Pages (JSP) script in the main web server root to execute arbitrary code with the permissions of the WebLogic installation.

Resolution

Apply the patch referenced in the Oracle Critical Patch Update - July 2012.

References

http://www.exploit-db.com/exploits/20318/

Limitations

This exploit was tested against Oracle Business Transaction Management 12.1.0.2.7 on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 (DEP OptOut).

The "Server Examples" component must be installed with Oracle WebLogic.

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **controlSoapBinding** service allows remote attackers to execute arbitrary commands by sending a request for the **createDataStore** method with a specially crafted **dataFiles** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **controlSoapBinding** service allows remote attackers to execute arbitrary commands by sending a request for the **createDataStore** method with a specially crafted **dataFiles** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **controlSoapBinding** service allows remote attackers to execute arbitrary commands by sending a request for the **createDataStore** method with a specially crafted **dataFiles** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

Oracle Endeca Server createDataStore method command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3763

Background

Oracle Endeca Server is a hybrid search-analytical database.

Problem

A vulnerability in the **`controlSoapBinding`** service allows remote attackers to execute arbitrary commands by sending a request for the **`createDataStore`** method with a specially crafted **`dataFiles`** parameter.

Resolution

Apply the patch referenced in the July 2013 Critical Patch Update.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-190/

Limitations

Exploit works on Oracle Endeca Server 7.4.0 on Windows Server 2008 R2 SP1 (DEP OptOut).

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

PHP Remote File Inclusion

Severity: Unsuccessful Exploit

Background

PHP scripts support the **`include`** and **`require`** statements, which cause an outside script to be run within the calling script. The included script can be a local file or, in some configurations, the URL of a remote file.

Problem

The PHP script is vulnerable to a remote file inclusion vulnerability. This vulnerability typically arises due to an **`include`** or **`require`** command where the included file path can be manipulated by a remote user via a specific HTTP input parameter. A remote attacker could execute arbitrary PHP commands on the target by specifying the URL of a PHP script on his or her own server in the input parameter.

Resolution

Fix the vulnerable code so that included path names cannot be manipulated by the user.

The vulnerability can also be mitigated by setting the following variables in the PHP configuration file:

```
register_globals = Off
allow_url_include = Off
safe_mode = On
```

References

http://projects.webappsec.org/Remote-File-Inclusion

Limitations

This exploit works against Unix and Linux operating systems.

The exploit requires the **`register_globals`** and **`allow_url_include`** PHP settings to be on, and the **`safe_mode`** PHP setting to be off.

The **`telnet`** and **`mkfifo`** programs must exist on the target in order for the shell connection to be established.

phpBB viewtopic.php highlight parameter vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2086

Background

phpBB is an open-source bulletin board package written in PHP.

Problem

This is a variant of an older vulnerability which allows remote command execution by requesting **`viewtopic.php`** with a specially crafted **`highlight`** parameter.

Resolution

Upgrade to the latest version of phpBB.

References

http://archives.neohapsis.com/archives/bugtraq/2005-06/0256.html

phpRPC decode function command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2006-1032

Background

phpRPC is an xmlrpc library written in PHP supporting most databases.

Problem

A vulnerability in the **decode** function allows a remote attacker to execute arbitrary PHP commands placed inside a **<base64>** tag.

Resolution

phpRPC is no longer maintained by the author, so no fix is available. If phpRPC is installed as part of another product, contact the vendor of that product for a fix. Otherwise, remove phpRPC from the server.

References

http://archives.neohapsis.com/archives/bugtraq/2006-02/0507.html

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

Plone Zope SAXutils Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-3587

Background

Plone is a free and open source content management system built on top of the Zope application server. Plone can be used for any kind of website, including blogs, internet sites, webshops and internal websites.

Problem

Plone fails to properly sanitize user-supplied input passed to cmd parameter in p_/webdav/xmltools/minidom /xml/sax/saxutils/os/popen2. This can be exploited to execute arbitrary shell commands.

Resolution

Upgrade to Plone 2.12.20 or 2.13.10 or apply patch Products.Zope_Hotfix_CVE_2011_3587.

References

http://plone.org/products/plone/security/advisories/20110928

Limitations

This exploit has been tested against Plone 4.1 on Fedora 13 Linux and Plone 4.0.9 on Ubuntu 10.04 LTS.

RSA Authentication Agent for Web for IIS chunked encoding overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1471

Background

RSA Authentication Agent For Web for IIS provides access control for applications on IIS web servers.

Problem

A heap overflow vulnerability when using chunked transfer-encoding allows remote attackers to execute arbitrary commands with LocalSystem privileges.

Resolution

A fix is available from https://knowledge.rsasecurity.com.

References

http://www.kb.cert.org/vuls/id/790533
http://archives.neohapsis.com/archives/vulnwatch/2005-q2/0039.html

Limitations

Exploit works on RSA Authentication Agent For Web for IIS 5.3 on Windows 2000 SP4.

The success of this exploit depends on the system state at the time the exploit is attempted.

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login

required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SAPHostControl Command Injection

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications.

Problem

The NetWeaver management console exposes an authenticated SOAP web service interface. During the authentication phase, user-supplied values within in the SOAP request are passed as parameters to a child process. In NetWeaver 7.02 and prior, the parameters are not properly validated and may allow an attacker to execute arbitrary commands on the server.

Resolution

An update is available through the SAP customer portal. Please see SAP Security Note 1341333 (login required).

References

http://www.contextis.com/research/blog/sap4/

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote

Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

Serv-U Web Client session cookie handling buffer overflow

Severity: Unsuccessful Exploit

Background

Serv-U is an FTP server for Windows platforms. The Serv-U Web Client component provides a browser-based interface to Serv-U.

Problem

A buffer overflow in the Serv-U Web Client allows remote attackers to execute arbitrary code when overly long session cookies are sent to the Web Client.

Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

References

http://www.rangos.de/ServU-ADV.txt

Limitations

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts DefaultActionMapper redirect Prefix Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2251

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities.

Problem

The **`DefaultActionMapper`** in Struts 2 versions prior to 2.3.15.1 does not properly handle parameters with a crafted **`redirect:`** prefix. This could allow remote attackers to execute arbitrary OGNL code.

Resolution

Upgrade to Struts 2.3.15.1 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-016.html

Limitations

This exploit was tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Apache Struts URL includeParams Attribute OGNL Code Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2013-2115

Background

Apache Struts is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model-view-controller (MVC) architecture.

Problem

Struts uses Object-Graph Navigation Language (OGNL) to provide extensive expression evaluation capabilities. Struts 2 versions prior to 2.3.14.2 do not properly handle the includeParams attribute in URLs. This could allow remote attackers to execute arbitrary OGNL code via a crafted request.

Resolution

Upgrade to Struts 2.3.14.2 or higher.

References

http://struts.apache.org/development/2.x/docs/s2-014.html

Limitations

This exploit has been tested against Apache Software Foundation Struts 2.3.1.1 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

This exploit requires that the Struts Action URL be provided.

Sun Java System Web Server WebDAV OPTIONS request buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2010-0361

Background

Sun Java System Web Server is a web application server. WebDAV (Web-based Distributed Authoring and Versioning) is an extension to the HTTP protocol which allows users to edit web server content.

Problem

A buffer overflow vulnerability in Sun Java System Web Server's WebDAV implementation allows remote attackers to execute arbitrary commands by sending a specially crafted OPTIONS request.

Resolution

Upgrade to Sun Java System Web Server 6.1 Service Pack 12 or 7.0 Release 8 or higher.

References

http://secunia.com/advisories/38260/
http://sunsolve.sun.com/search/document.do?assetkey=1-66-275850-1

Limitations

Exploit works on Sun Java System Web Server 7.0 Update 7 on Windows Server 2003 SP2 with patch KB933729.

WebDAV support must be enabled on the target in order for the exploit to succeed, and the correct WebDAV URI must be specified.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

Symantec Endpoint Protection Manager XXE and SQL Injection Vulnerabilities

Severity: Unsuccessful Exploit **CVE:** CVE-2013-5014

Background

Symantec Endpoint Protection, by Symantec Corporation, is an antivirus and personal firewall product designed to be centrally managed in corporate environments by the Symantec Endpoint Protection Manager (SEPM). The SEPM management console listens on TCP port 9090.

Problem

The management console for Symantec Endpoint Protection Manager is vulnerable to External XML Entity (XXE) injection (CVE-2013-5014) due to improper sanitization of external XML data. This vulnerability could potentially allow unauthorized access to restricted server-side data and console management functionality. Symantec Endpoint Protection Manager's management console is also vulnerable to SQL injection (CVE-2013-5015) due to insufficient sanitization of local queries made against the backend database. The XXE injection vulnerability can be leveraged to exploit the local access SQL injection vulnerability.

Resolution

Apply the updates as described in Symantec Security Advisory SYM14-004.

References

http://www.zdnet.com/attackers-scanning-for-symantec-endpoint-protection-manager-flaw-7000026418/
http://secunia.com/advisories/cve_reference/CVE-2013-5014/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5015
http://secunia.com/advisories/cve_reference/CVE-2013-5015/
http://osvdb.org/show/osvdb/103306

Limitations

This exploit was tested against the default Symantec Endpoint Protection Manager installation using embedded database on Windows Server 2003.

TFTP Server error packet buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2161

Background

TFTP Server is an open source server implementation of the tftp protocol for multiple platforms.

Problem

A buffer overflow vulnerability in the handling of error packets allows remote attackers to execute arbitrary commands.

Resolution

Upgrade to version 1.6 or higher when available, if that version contains a fix. Otherwise restrict access to the tftp service.

References

http://www.milw0rm.com/exploits/5563

Limitations

Exploit works on TFTP Server SP 1.4.

A different payload is required depending upon whether the service runs as a network service or standalone. Choose the first platform if TFTP Server is running as a network service, and the second if it is running standalone.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **jhot.php** script allows remote attackers to upload arbitrary PHP commands into the **img/wiki** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **jhot.php** script allows remote attackers to upload arbitrary PHP commands into the **img/wiki** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **jhot.php** script allows remote attackers to upload arbitrary PHP commands into the **img/wiki** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

Traq authenticate function remote code execution

Severity: Unsuccessful Exploit

Background

Traq is a PHP5+ and MySQL4+ based Project Tracking system with the ability to host multiple projects.

Problem

The flaw is caused due to admin rights not properly being restricted in the "authenticate()" function in admincp/common.php. This can be exploited to execute arbitrary code.

Resolution

Upgrade to Traq 2.3.1 or later.

References

http://www.exploit-db.com/exploits/18213
http://secunia.com/advisories/47108

Limitations

This exploit has been tested against Traq 2.3 on Linux.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-2437

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in **`cgiRecvFile.exe`** allows remote attackers to execute arbitrary commands by sending an HTTP request containing a specially crafted **`ComputerName`** parameter.

Resolution

Apply the appropriate patch.

References

http://secunia.com/secunia_research/2008-35/

Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

Trend Micro OfficeScan Policy Server CGI buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-1365

Background

Trend Micro OfficeScan is a centralized virus and security scan management system.

Problem

A buffer overflow vulnerability in the Policy Server for Cisco NAC component allows remote attackers to execute arbitrary commands by sending a long, specially crafted **pwd** parameter to the **cgiABLogon.exe** CGI program.

Resolution

Restrict access to the OfficeScan HTTP port.

References

http://secunia.com/advisories/29124/

Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **rev** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **rev** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **rev** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **rev** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **rev** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **rev** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be

exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2008-4008

Background

Oracle WebLogic Server (formerly BEA WebLogic Server) is a Java web application platform.

Problem

A buffer overflow vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted Transfer-Encoding header in an HTTP request.

Resolution

Install the latest WebLogic Server plug-in referenced in the Oracle Security Advisory.

References

https://support.bea.com/application_content/product_portlets/securityadvisories/2806.html

Limitations

Exploit works on the WebLogic Server Connector for Apache 1.0.1136334.

WhatsUp Gold _maincfgret.cgi instancename buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0798

Background

WhatsUp Professional (formerly WhatsUp Gold) is a network mapping and monitoring tool.

Problem

A buffer overflow in the WhatsUp Gold web interface allows remote command execution by requesting **`_maincfgret.cgi`** with a long **`instancename`** parameter.

Resolution

Install WhatsUp Gold 8.03 Hotfix 1.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=133&type=vulnerabilities

Limitations

Exploit works on Ipswitch WhatsUp Gold 8.03.

Successful exploitation requires valid user credentials with permissions to *Configure Program* and *Configure Reports*.

Note that the WhatsUp Gold installation path may affect the success of this exploit. The exploit is designed to work with the default installation path only.

Windows Plug and Play buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-1983

Background

The Windows Plug and Play service allows Windows operating systems to automatically detect and configure a new hardware device, such as a mouse.

Problem

A buffer overflow in the Plug and Play service could allow command execution with administrative privileges.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 05-047.

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Limitations

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

Windows Workstation service NetpManageIPCConnect buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4691

Background

The Windows Workstation service routes network requests for file or printer resources.

Problem

A buffer overflow in the NetpManageIPCConnect function in the Windows Workstation service allows command execution when a domain join request causes communication with a malicious domain controller.

Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

Wireshark DECT Dissector Remote Stack Buffer Overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2011-1591

Background

Wireshark is a network packet analyzer.

Problem

A buffer overflow vulnerability in the DECT dissector allows command execution when a user sends a specially crafted datagram over a network which is being analyzed by Wireshark.

Resolution

Upgrade to Wireshark 1.4.5 or higher.

References

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Limitations

Exploit works on Wireshark 1.4.4.

The affected target running Wireshark must be on the same network as as the SAINTexploit host.

Exploit requires the Net-Write PERL module to be installed on the scanning host. This module is available from http://search.cpan.org/dist/Net-Write/lib/Net/Write.pm.

The "Wireshark DECT Dissector PCAP File Processing Overflow" client exploit attempts to exploit the same vulnerability. The client exploit does not have the same network and PERL module limitations, but requires user cooperation.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

Xi Software Net Transport eDonkey Protocol Buffer Overflow

Severity: Unsuccessful Exploit

Background

Net Transport, also known as NetXfer, is a download manager for Windows made by Xi Software. Among the protocols Net Transport can handle is eDonkey, a decentrailized peer to peer network for file sharing.

Problem

The Net Transport download manager fails to properly sanitize user input from the eDonkey network, specifically in processing eDonkey **`OP_LOGINREQUEST`** packets. A successful attacker sending a specially crafted packet could cause a stack buffer overflow and execute arbitrary code.

Resolution

Restrict access to the port used for eDonkey. Upgrade to a newer version of Net Transport that contains a fix.

References

http://secunia.com/advisories/38028/

Limitations

Exploit runs on Xi Software Net Transport 2.90.510.
The eDonkey service port must be known by the attacker. By default, the application uses a random port.
The exploit may take a longer time to establish a shell connection.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841

http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2010-4229

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 10.3 prior to 10.3.2 and version 11 fail to validate the name of uploaded files. An attacker may exploit this behavior to upload an executable Java file

while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Upgrade to ZENworks 10.3.2 or later.

References

http://www.novell.com/support/viewContent.do?externalId=7007841
http://zerodayinitiative.com/advisories/ZDI-11-118/

Limitations

This exploit has been tested against Novell ZENworks Configuration Management 10.3 running on Microsoft Windows Server 2003 SP2 English (DEP OptOut) and Microsoft Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote

shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Asset Management rtrlet File Upload Traversal

Severity: Unsuccessful Exploit **CVE:** CVE-2011-2653

Background

Novell ZENworks is a resource management solution consisting of a management server and management agents.

Problem

The Asset Management module (ZAM) of ZENworks version 7.5 fails to validate the name of uploaded files via POST requests to the /rtrlet/ resource. An attacker may exploit this behavior to upload an executable Java file while traversing the directory structure, such that the uploaded file will be executed by the server.

Resolution

Apply the vendor supplied patch.

References

http://www.zerodayinitiative.com/advisories/ZDI-11-342/

Limitations

This exploit has been tested against Novell ZENworks Asset Management 7.5 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 English (DEP OptOut). The exploit may not execute immediately. It may take 15 seconds or more before the payload is executed. This exploit creates a remote shell web application named 'exploit' on the webserver. This application remains after the connection is closed and must be manually removed.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Configuration Management UploadServlet Remote Code Execution

Severity: Unsuccessful Exploit

Background

Novell ZENworks Configuration Management is an IT desktop computer management suite that provides the ability to install, configure and administer desktop computers from a centralized location. The product is based on a client/server architecture.

Problem

A remote code execution vulnerability exists in Novell ZENworks Configuration Management 10.x prior to 10.3. The vulnerability is due to insufficient input validation within the ZENworks Server's UploadServlet. Remote unauthenticated attackers can leverage this vulnerability to upload malicious files anywhere onto the target server.

Resolution

Upgrade to Novell ZENworks Configuration Managment 10.3.

References

http://secunia.com/advisories/39212/

Limitations

Exploit works on Novell ZENworks Configuration Management 10.2.0.
Because it takes time for the affected server to deploy the malicious file sent by the attacker, the exploit script has a 10-second pause during the attack. Thus it will take longer time than normal to establish the shell session.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to

disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management DUSAP.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1082

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.0 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`DUSAP.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.novell.com/support/kb/doc.php?id=7011896
http://www.zerodayinitiative.com/advisories/ZDI-13-088/

Limitations

This exploit was tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language

parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

Novell ZENworks Mobile Management MDM.php Language Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1081

Background

ZENworks Mobile Management (ZMM) offers centralized management tools that are useful for deploying new mobile devices in the workforce, whether those devices are company-issued or privately owned. ZMM ensures that users have the right credentials and access levels for company e-mail, calendar and contacts, as well as the right applications and files for each device. ZMM can also track device usage and the applications that users download onto their devices.

Problem

Novell ZMM 2.7.1 and 2.6.1, and probably earlier versions, are vulnerable to local file inclusion via a directory

traversal style attack which could allow a remote unauthenticated attacker to execute arbitrary commands or code. The issue is due to the **`MDM.php`** script not properly sanitizing user input supplied to the language parameter, thereby allowing an attacker to include a file from the targeted host that could contain arbitrary commands or code that will be executed by the vulnerable script. In addition, this flaw could be used to disclose the contents of any file on the system accessible by the web server via **`require_once()`**.

Resolution

Upgrade to Novell ZMM 2.7.1 when available.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-087/
http://www.novell.com/support/kb/doc.php?id=7011895

Limitations

This exploit has been tested against Novell ZENworks Mobile Management 2.6.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP2 (DEP OptOut).

The Perl module **`MIME::Base64`** is required to run the exploit.

1026/TCP

Severity: Service

1027/TCP

Severity: Service

1029/TCP

Severity: Service

1033/TCP

Severity: Service

1039/TCP

Severity: Service

1044/TCP

Severity: Service

9389/TCP

Severity: Service

DNS

Severity: Service

NFS

Severity: Service

SMB

Severity: Service

WWW

Severity: Service

WWW (Secure)

Severity: Service

WWW (non-standard port 5985)

Severity: Service

WWW (non-standard port 8059)

Severity: Service

WWW (non-standard port 8082)

Severity: Service

blackjack (1025/TCP)

Severity: Service

cma (1050/TCP)

Severity: Service

domain (53/UDP)

Severity: Service

epmap (135/TCP)

Severity: Service

http-rpc-epmap (593/TCP)

Severity: Service

iad1 (1030/TCP)

Severity: Service

iad2 (1031/TCP)

Severity: Service

iscsi-target (3260/TCP)

Severity: Service

kerberos (88/TCP)

Severity: Service

kpasswd (464/TCP)

Severity: Service

ldap (389/TCP)

Severity: Service

m4-network-as (4345/TCP)
Severity: Service

microsoft-ds (445/TCP)
Severity: Service

ms-wbt-server (3389/TCP)
Severity: Service

msft-gc (3268/TCP)
Severity: Service

msft-gc-ssl (3269/TCP)
Severity: Service

neod1 (1047/TCP)
Severity: Service

neod2 (1048/TCP)
Severity: Service

netbios-ns (137/UDP)
Severity: Service

obrpd (1092/TCP)
Severity: Service

proofd (1093/TCP)
Severity: Service

shilp (2049/TCP)
Severity: Service

ssl-ldap (636/TCP)
Severity: Service

sunrpc (111/TCP)
Severity: Service

tftp (69/UDP)
Severity: Service

unicall (4343/TCP)
Severity: Service

4.8 10.8.0.230

IP Address: 10.8.0.230
Scan time: Dec 14 12:43:41 2015

Host type: Linux 3.13.0-57-generic - Ubuntu 14.04
Netbios Name: UBUNTUNESSUS

Windows password weakness (nobody:)

Severity: Remote Administrator **CVE:** CVE-1999-0503

Background

Passwords are the most commonly used method of authenticating users to a server. The combination of a login name and password is used to verify the identity of a user requesting access, and to determine what parts of the server the user has permission to access.

Problem

Administrators often set up new user accounts with no password or with a default password which is easy to guess. Additionally, some users may choose a simple password which is easy to remember. Null passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system.

Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

References

http://www.securityfocus.com/infocus/1537

Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

ALCASAR index.php Crafted HTTP host Header Vulnerability

Severity: Unsuccessful Exploit

Background

ALCASAR is a free Network Access Controller that allows network managers to restrict Internet service access to authenticated users. ALCASAR allows control and logging of all network activity by users and/or defined user groups.

Problem

ALCASAR 2.8 and earlier are vulnerable to remote code execution by injecting the **`exec()`** function into the HTTP host header to gain access as the Apache user. By also exploiting the Apache user's sudoer capability with **`openssl`**, a remote attacker could leverage the origial vulnerability to gain root privileges.

Resolution

ALCASAR 2.8.1 purportedly fixes the host header vulnerability.

References

http://seclists.org/fulldisclosure/2014/Sep/26

Limitations

Exploit works on ALCASAR 2.8.

The **`MIME::Base64`** module is required on the SAINTexploit host.

Exploit only results in Apache permissions, not root permissions.

AWStats migrate parameter command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2237

Background

AWStats is a web application for showing web, FTP, and mail server statistics.

Problem

AWStats uses the value of the **`migrate`** input parameter in a PERL *open* call without sufficient checks for invalid characters, allowing remote command execution.

Resolution

Upgrade to AWStats 6.6 or higher, or disable the **`AllowToUpdateStatsFromBrowser`** option in the AWStats configuration file.

References

http://secunia.com/advisories/19969

BASE base_qry_common.php file include

Severity: Unsuccessful Exploit **CVE:** CVE-2006-2685

Background

Snort is an open-source intrusion detection system. The Basic Analysis and Security Engine (BASE) is a web interface for analyzing Snort results.

Problem

If the register_globals PHP option is enabled, the **`base_qry_common.php`** script can be used to include arbitrary files under the directory specified by the **`BASE_path`** parameter. This could lead to execution of local or remote PHP code.

Resolution

Upgrade to BASE 1.2.5 or higher.

References

http://secunia.com/advisories/20300

Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

Bash environment variable code injection over HTTP

Severity: Unsuccessful Exploit **CVE:** CVE-2014-6271

Background

GNU Bash (Bourne Again SHell) is a command shell commonly used on Linux and Unix systems.

Problem

The Bash shell executes commands injected after function definitions contained in environment variables. This could be used by a remote attacker to cause arbitrary commands to execute if a web server hosts programs which invoke the Bash shell.

Resolution

Apply updated Bash packages from the Linux or Unix vendor.

References

https://www.us-cert.gov/ncas/alerts/TA14-268A

Limitations

This exploit requires the path to a web program which invokes the Bash shell. This attack vector may not exist on all systems with affected versions of Bash, and other attack vectors may exist which are not covered by this exploit.

Cisco IOS HTTP exec path command execution

Severity: Unsuccessful Exploit **CVE:** CVE-2000-0945

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands through HTTP requests by requesting a path beginning with **`/exec`**.

Resolution

Set an enable password on the Cisco device.

References

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

Limitations

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

Cisco IOS HTTP access level authentication bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2001-0537

Background

The Cisco Internetwork Operating System (IOS) is the operating system used by Cisco routers.

Problem

A remote attacker could execute arbitrary commands at the highest privilege level (level 15) without needing to authenticate by requesting a URL of the form **`http://target/level/xx/exec/command`**, where *xx* is some number between 16 and 99.

Resolution

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

References

http://www.cert.org/advisories/CA-2001-14.html

Limitations

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

CS-MARS JBoss jmx-console access

Severity: Unsuccessful Exploit **CVE:** CVE-2006-3733

Background

The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) recognizes and correlates network attacks.

Problem

CS-MARS includes the JBoss web application server with insufficient access control to the **`jmx-console`** component. This component can be used by a remote attacker to execute arbitrary commands.

Resolution

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

References

http://www.securityfocus.com/archive/1/440641

D-Link Cookie command injection

Severity: Unsuccessful Exploit

Background

D-Link produces a variety of routers, switches, and other network equipment for home users and businesses.

Problem

A command injection vulnerability allows remote attackers to execute arbitrary commands by sending a specially crafted cookie in an HTTP request.

Resolution

Apply a firmware upgrade which fixes this vulnerability when one becomes available.

References

https://github.com/darkarnium/secpub/tree/master/D-Link/DSP-W110

Limitations

Exploit works on D-Link DSP-W110 (Rev A) - v1.05b01.

JRun mod_jrun WriteToLog buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2004-0646

Background

Macromedia JRun is a J2EE application server. mod_jrun is an Apache module which enables the use of JRun applications through an Apache web server.

Problem

A buffer overflow vulnerability in mod_jrun and mod_jrun20 allows a remote attacker to execute arbitrary commands on the web server if verbose logging is enabled.

Resolution

Apply the patch referenced in Macromedia Security Bulletin 04-08.

References

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=145&type=vulnerabilities

Limitations

Exploit works on JRun 4 SP1a with verbose logging enabled.

Nagios statuswml.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2009-2288

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `statuswml.cgi` script passes unsanitized data to the `ping` and `traceroute` commands, resulting in shell command execution via metacharacters. A successful remote attacker could use a specially crafted request to execute arbitrary commands.

Resolution

Upgrade to Nagios 3.1.1 or later.

References

http://secunia.com/advisories/35543/

Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

Nagios XI Graph Explorer Component OS Command Injection Vulnerability

Severity: Unsuccessful Exploit

Background

Nagios XI is a network host and service monitoring and management system.

Problem

Nagios XI Graph Explorer Component is vulnerable to arbitrary command execution by authenticated users. The vulnerability is due to the `visApi.php` script not sanitizing user-supplied input to the 'host' parameter.

Resolution

Upgrade to Nagios Graph Explorer SVN 1.3.

References

http://secunia.com/advisories/49749/

Limitations

This exploit has been tested against Nagios Enterprises Nagios XI 2011r1.9 on CentOS Project CentOS 6 with Exec-Shield Enabled.

This exploit requires valid Nagios web interface login credentials.

The Netcat (nc) utility tool must be installed on the target.

Nagios 3 history.cgi Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2012-6096

Background

Nagios is a network host and service monitoring and management system.

Problem

The Nagios `history.cgi` script is vulnerable to a stack overflow when parsing the `host` parameter. This may allow an attacker to execute arbitrary code on the target system under the context of the Nagios webserver process.

Resolution

Upgrade to Nagios 3.4.4 or later.

References

http://lists.grok.org.uk/pipermail/full-disclosure/2012-December/089125.html
https://dev.icinga.org/issues/3532
https://www.icinga.org/2013/01/14/icinga-1-6-2-1-7-4-1-8-4-released/

Limitations

This exploit has been tested against Nagios Enterprises Nagios 3.4.3 on CentOS 6 (Exec-Shield Enabled).
This exploit creates an executable file in /tmp/x which should be manually removed after successful exploitation. As such, this exploit also requires /tmp to be mounted without the `noexec` flag.
This exploit requires the `base64` utility to be installed on the system.

PHP CGI Query String Parameters Command Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1823

Background

PHP is a widely used general-purpose scripting language that is especially suited for Web development.

Problem

When configured as a CGI script (aka php-cgi), PHP does not properly handle query string parameters which are passed directly to the php-cgi program. This can be exploited to execute arbitrary system commands or disclose the PHP source code.

Resolution

Upgrade PHP to version 5.4.3 or 5.3.13 or higher.

References

http://secunia.com/advisories/49014
http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823

Limitations

This exploit has been tested against PHP 5.3.10 on Windows XP SP3 and PHP 5.4.0 on Ubuntu 11.10 Linux.

phpMyAdmin preg_replace from_prefix sanitization vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3238

Background

phpMyAdmin is a free software tool, written in PHP, designed to handle the administration of MySQL over the Web.

Problem

phpMyAdmin before 3.5.8.1 is vulnerable to code injection as a result of failure to sanitize input passed via the **`from_prefix`** parameter passed to **`preg_replace()`** in **`libraries/mult_submits.inc.php`**. As a result, an authenticated remote attacker could potentially execute arbitrary code.

Resolution

Upgrade to phpMyAdmin 3.5.8.1 or newer.

References

http://www.phpmyadmin.net/home_page/security/PMASA-2013-2.php

Limitations

This exploit was tested against phpMyAdmin Devel Team phpMyAdmin 3.5.8 on CentOS 6 (with Exec-Shield Enabled).

Netcat (nc) must be installed on the target.

Exploit requires a valid path to phpMyAdmin and valid user credentials for phpMyAdmin's web interface.

Only phpMyAdmin running on a PHP version before 5.4.7 is vulnerable. Newer PHP versions will generate a warning.

PineApp Mail-SeCure ldapsyncnow.php command injection

Severity: Unsuccessful Exploit

Background

PineApp Mail-SeCure is an e-mail security appliance which provides perimeter security protection to stop

threats prior to their penetration of the customer's network, as well as post-perimeter anti-spam content inspection.

Problem

A vulnerability in PineApp Mail-SeCure allows remote attackers to execute arbitrary commands contained in the **`shell_command`** parameter in a request for the **`ldapsyncnow.php`** script.

Resolution

Restrict access to ports 7080 and 7443.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-185/

Limitations

Exploit works on PineApp Mail-SeCure 3.70 running on PineApp Linux 3.0.53.

PineApp Mail-SeCure test_li_connection.php Command Injection

Severity: Unsuccessful Exploit

Background

PineApp Mail-SeCure is an e-mail security appliance which provides perimeter security protection to stop threats prior to their penetration of the customer's network, as well as post-perimeter anti-spam content inspection.

Problem

PineApp Mail-SeCure is vulnerable to arbitrary command injection as a result of failure to properly sanitize user-supplied data in the test_li_connection.php component. An unauthenticated remote attacker could leverage this vulnerability to execute arbitrary code with root privileges.

Resolution

Contact the vendor for an update when one becomes available. In the interim, restrict access to ports 7443 and 7080 of the PineApp device or VM to those machines which have a legitimate need to access the PineApp software directly.

References

http://www.zerodayinitiative.com/advisories/ZDI-13-188/
http://secunia.com/advisories/54342/

Limitations

This exploit has been tested against PineApp Mail-SeCure 3.70 on PineApp Linux 3.0.53.

The Perl module **`MIME::Base64`** is required to run the exploit.

Samba call_trans2open buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2003-0201

Background

Samba is a software package which implements the SMB protocol on a variety of platforms, providing compatibility with Windows systems.

Problem

A buffer overflow in the **`call_trans2open`** function allows anonymous remote attackers to execute arbitrary commands.

Resolution

Upgrade to Samba 2.2.8a or higher.

References

http://www.kb.cert.org/vuls/id/267873
http://archives.neohapsis.com/archives/bugtraq/2003-04/0100.html

Limitations

Exploit works on Samba 2.2.x.

Samba lsa_io_trans_names buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2007-2446

Background

Samba is a software package which implements the SMB protocol on a variety of platforms, providing compatibility with Windows systems.

Problem

A vulnerability in the LSA RPC interface allows a remote attacker to execute arbitrary commands by sending a specially crafted **`LsarLookupSids/LsarLookupSids2`** request, which causes a buffer overflow in the **`lsa_io_trans_names`** function.

Resolution

Upgrade to Samba 3.0.25 or higher, apply the patch for Samba 3.0.24, or apply the patch for Solaris.

References

http://www.zerodayinitiative.com/advisories/ZDI-07-033.html
http://us1.samba.org/samba/security/CVE-2007-2446.html

Limitations

Exploit works on Samba 3.0.24 on Sun SPARC Solaris 9 and Samba 3.0.22 on SuSE Linux Enterprise Server 10.

Since the exploit uses a brute force method, extra time may be required before the exploit succeeds.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for this exploit. These packages are available from http://cpan.org/modules/by-module/.

SAP NetWeaver SOAP RFC SXPG_CALL_SYSTEM Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

SAP NetWeaver 7.02 and earlier contains a flaw in the SAP SOAP RFC service SXPG_CALL_SYSTEM command when configured with transaction SM69. This may allow a remote authenticated attacker to manipulate certain parameters related to the command and execute other, arbitrary commands.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://www.osvdb.org/show/osvdb/93537

Limitations

This exploit has been tested against SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 English (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1.

Valid credentials (user name and password) to the application's web interface (with privileges to use the SAP SOAP RFC) and a valid client ID must be provided to the exploit script.

The Perl module **`MIME::Base64`** is required to run the exploit.

Wget utility tool must be installed on the target on Linux.

IPv6 is only fully supported for the exploit on Windows targets.

SAP NetWeaver SOAP RFC SXPG_COMMAND_EXECUTE Command Execution

Severity: Unsuccessful Exploit

Background

SAP NetWeaver is a technology platform for building and integrating SAP business applications. Remote Function Call (RFC) is the standard SAP interface for communication between SAP systems. Transaction SM69 is used to create and maintain external operating system commands.

Problem

A vulnerability in the SXPG_COMMAND_EXECUTE Remote Function Call allows a remote, authenticated attacker to execute arbitrary commands by sending a command that is configured with transaction SM69 containing specially crafted arguments.

Resolution

Obtain an update at the SAP Customer Portal (login required).

References

http://osvdb.org/93536

Limitations

Exploit works on SAP NetWeaver 7.02 SP06 on Windows Server 2003 SP2 (DEP OptOut), Windows Server 2008 SP2 (DEP OptOut), and SUSE Linux Enterprise Server 11 (x86_64) SP1 and requires a valid user's credentials to the application's web interface.

A valid client ID must be specified.

The Perl module 'MIME::Base64' is required to run the exploit.

The wget utility must be installed on Linux targets.

IPv6 is only supported for Windows targets.

Snort Back Orifice Pre-Processor buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2005-3252

Background

Back Orifice is a remote system administration program for Windows. It is commonly installed by attackers or Trojan Horse programs for use as a backdoor.

Snort is an open-source intrusion detection system. It includes a Back Orifice pre-processor, which handles Back Orifice traffic before it is passed to the intrusion detection engine.

Problem

A buffer overflow vulnerability in the Back Orifice pre-processor in Snort could allow remote attackers to execute arbitrary commands by sending a specially crafted Back Orifice ping to a host on a network monitored by Snort.

Resolution

Upgrade to Snort 2.4.3 or higher.

References

http://www.kb.cert.org/vuls/id/175500

Limitations

Exploit works on Snort 2.4.2 on Windows and Red Hat 8.

Snort DCE/RPC preprocessor buffer overflow

Severity: Unsuccessful Exploit **CVE:** CVE-2006-5276

Background

Snort is an open-source intrusion detection system. It includes a DCE/RPC preprocessor, which reassembles DCE/RPC traffic before it is passed to the intrusion detection engine.

Problem

A buffer overflow vulnerability in the DCE/RPC preprocessor allows remote attackers to execute arbitrary commands by chaining together multiple **`WriteAndX`** requests in the same TCP segment.

Resolution

Upgrade to Snort 2.6.1.3 or higher.

References

http://www.us-cert.gov/cas/techalerts/TA07-050A.html
http://www.snort.org/docs/advisory-2007-02-19.html

Limitations

Exploit works on Snort 2.6.1.1 on Windows and Snort 2.6.1.2 on Red Hat 8, and requires port 445/TCP to be open on the target.

SonicWall Multiple Products skipSessionCheck Authentication Bypass

Severity: Unsuccessful Exploit **CVE:** CVE-2013-1359

Background

Dell SonicWALL has several management and reporting solutions which provide a centralized architecture for creating and managing security policies, providing real-time monitoring and alerts, and delivering compliance and usage reports from a single management interface. These products include SonicWALL ViewPoint (being discontinued and replaced by SonicWALL Analyzer), Global Management System (GMS), and the Universal Management Appliance (UMA).

Problem

Various versions of Dell SonicWALL ViewPoint, Analyzer, GMS and UAM contain an error within the authentication mechanism of the web interface which can be exploited to bypass the authentication mechanism by setting the **`skipSessionCheck`** parameter to 1.

Resolution

Obtain HotFix 125076.77 from http://www.mysonicwall.com and apply the appropriate files for your product.

References

http://secunia.com/advisories/51758/

Limitations

This exploit was tested against SonicWALL GMS 7.0 SP1 on Windows Server 2003 SP2 English and Windows Server 2008 SP2 (with DEP OptOut). It was also tested against SonicWALL GMS Virtual Appliance 7.0 SP1 on SonicWALL Linux 2.6.23.8.

This exploit supports IPv6 on Windows platforms, but not on GMS Virtual Appliance platforms.

Splunk Search Jobs Remote Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2011-4642

Background

Splunk collects, indexes and harnesses the massive volumes of valuable machine data generated by your complex IT infrastructure, whether physical, virtual or in the cloud.

Problem

Splunk allows users to perform search actions via HTTP requests without performing proper validity checks to verify the requests. This can be exploited to execute arbitrary command/code when a logged-in administrator visits a specially crafted web page.

Resolution

Upgrade to Splunk 4.2.5 or later.

References

http://www.sec-1.com/blog/?p=233
http://www.exploit-db.com/exploits/18245/
http://www.sec-1.com/blog/wp-content/uploads/2011/12/Attacking_Splunk_Release.pdf

Limitations

This exploit has been tested against Splunk 4.2.4 build 110225 on Windows XP SP3 and Ubuntu 10.04 Linux.

F5 BIG-IP SSH private key

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1493

Background

SSH Private keys are used for authentication for many F5 BIG-IP devices. Devices shipped with a default, static key are vulnerable to compromise if the public discovers the key. The private key can be re-used by an attacker to gain remote, privileged access to the device.

Problem

Vulnerable BIG-IP installations allow unauthenticated users to bypass authentication and login as the 'root' user on the following devices:

- VIPRION B2100, B4100, and B4200
- BIG-IP 520, 540, 1000, 2000, 2400, 5000, 5100, 1600, 3600, 3900, 6900, 8900, 8950, 11000, and 11050
- BIG-IP Virtual Edition
- Enterprise Manager 3000 and 4000

Resolution

The vendor has indicated these versions are patched:

- 9.4.8-HF5 and later
- 10.2.4 and later
- 11.0.0-HF2 and later
- 11.1.0-HF3 and later

Note: Systems that are licensed to run in Appliance mode on BIG-IP version 10.2.1-HF3 or later are not susceptible to this vulnerability. For more information about Appliance mode, refer to SOL12815: Overview of Appliance mode.

References

http://support.f5.com/kb/en-us/solutions/public/12000/800/sol12815.html

Limitations

The target must be running the ssh service in order for the exploit to succeed.

The OpenSSH client must be installed on the SAINTexploit host.

Symantec Messaging Gateway Default SSH Password

Severity: Unsuccessful Exploit **CVE:** CVE-2012-3579

Background

Symantec Messaging Gateway is an email virus protection appliance that also provides antispam protection.

Problem

Symantec Messaging Gateway versions before 10.0 have a default password for the "support" account, which can be used to login remotely to the SSH service, and then gain privileged access.

Resolution

Upgrade to Symantec Messaging Gateway 10.0 or higher.

References

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120827_00

Limitations

Exploit works against Symantec Messaging Gateway 9.5.3-3 on platform CentOS Project CentOS 5.0 with Exec-Shield Enabled.

The OpenSSH client must be installed on the SAINTexploit host.

Symantec Web Gateway access_log PHP Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2012-0297

Background

Symantec Web Gateway protects organizations against multiple types of Web-based malware and prevents data loss over the Web.

Problem

Symantec Web Gateway fails to properly sanitize user-supplied input passed to "/spywall/releasenotes.php" via the "relfile" parameter. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade Symantec Web Gateway to version 5.0.3 or higher.

References

http://secunia.com/advisories/49216
http://www.symantec.com/security_response/securityupdates
/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120517_00

Limitations

This exploit has been tested against Symantec Web Gateway 5.0.0.216 and 5.0.2.8

Symantec Web Gateway pbcontrol.php Command Injection

Severity: Unsuccessful Exploit **CVE:** CVE-2012-2953

Background

Symantec Web Gateway protects organizations against multiple types of Web-based malware and prevents data loss over the Web.

Problem

Symantec Web Gateway 5.0.x.x before 5.0.3.18 is vulnerable to command injection due to `spywall/pbcontrol.php` failing to properly sanitize input passed via the `filename` parameter. This may allow a remote attacker to execute arbitrary shell commands.

Resolution

Upgrade to Symantec Web Gateway 5.0.3.18 or later with the Database Update 5.0.0.438 or later.

References

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20120720_00

Limitations

This exploit was tested against Symantec Web Gateway 5.0.0.216 on Fedora Project Fedora Core 3 with Exec-Shield Enabled.

TikiWiki file upload vulnerability (jhot.php)

Severity: Unsuccessful Exploit **CVE:** CVE-2006-4602

Background

TikiWiki is a multi-purpose web content management system written in PHP.

Problem

The **`jhot.php`** script allows remote attackers to upload arbitrary PHP commands into the **`img/wiki`** directory. The commands can then be executed by requesting the uploaded PHP file from a web browser.

Resolution

Upgrade to TikiWiki 1.9.5 or higher.

References

http://secunia.com/advisories/21733

TWiki revision control shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2005-2877

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The revision control function in TWiki does not sufficiently check the **`rev`** parameter before using it in a shell command call. This allows remote attackers to execute arbitrary commands using a **`rev`** parameter containing shell metacharacters.

Resolution

Apply the patch referenced in CIAC Bulletin P-307.

References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

TWiki Search.pm shell command injection

Severity: Unsuccessful Exploit **CVE:** CVE-2004-1037

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The Search.pm module does not sufficiently check search strings for illegal characters, allowing remote attackers to execute commands using search strings containing single-quote and backtick characters.

Resolution

Apply the update referenced in CIAC Bulletin P-039.

References

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

TWiki View Script debugenableplugins Request Parameter Vulnerability

Severity: Unsuccessful Exploit **CVE:** CVE-2014-7236

Background

TWiki is a web-based collaboration platform written in PERL.

Problem

The TWiki view script does not properly sanitize the **`debugenableplugins`** parameter before using it.

Resolution

Upgrade to TWiki-6.0.1 or higher, or apply the hotfix shown in the TWiki Security Alert.

References

http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2014-7236

Limitations

Exploit works on vulnerable TWiki installations that do not require authentication. If the protocol is https, exploit requires the IO::Socket::SSL Perl module to be installed on the SAINTexploit host. This module is available from http://www.cpan.org/modules/by-module/IO/.

vTiger CRM AddEmailAttachment arbitrary file upload

Severity: Unsuccessful Exploit **CVE:** CVE-2013-3214

Background

vTiger CRM is a customer relationship management application written in PHP.

Problem

An arbitrary file upload vulnerability when handling SOAP AddEmailAttachment requests allows remote attackers to execute arbitrary commands by uploading PHP scripts under the web root.

Resolution

Upgrade to version 6.0 when available, or apply the patch. Note that the patch only prevents exploitation by unauthenticated attackers.

References

http://seclists.org/bugtraq/2013/Aug/7

Limitations

Exploit works on vTiger CRM 5.4.0.

WebCalendar Pre-Auth PHP Code Execution

Severity: Unsuccessful Exploit **CVE:** CVE-2012-1495

Background

WebCalendar is a PHP-based calendar application that can be configured as a single-user calendar, a multi-user calendar for groups of users, or as an event calendar viewable by visitors.

Problem

WebCalendar fails to properly sanitize user-supplied input passed via the install/index.php script. This can be exploited to execute arbitrary PHP code.

Resolution

Upgrade WebCalendar to version 1.2.5 or higher.

References

http://www.k5n.us/webcalendar.php

Limitations

This exploit has been tested against WebCalendar 1.2.4 on Ubuntu 10.04 Linux.

WP Symposium Plugin for WordPress Arbitrary File Upload

Severity: Unsuccessful Exploit **CVE:** CVE-2014-10021

Background

WP Symposium is a social network plugin for WordPress.

Problem

WP Symposium Plugin for WordPress contains a vulnerability that allows a remote attacker to execute arbitrary PHP code. This vulnerability is due to the /wp-symposium/server/file_upload_form.php script not

properly verifying user-uploaded files and placing the files in a user-accessible location. A successful attacker can execute the uploaded script with the privileges of the web server.

Resolution

Upgrade the WP Symposium plugin when a fix is available. WP Symposium 14.12 has been released and is presumed to contain a fix.

References

http://www.exploit-db.com/exploits/35543/

Limitations

Exploit works on WP Symposium 14.11.

DNS

Severity: Service

SMB

Severity: Service

SSH

Severity: Service

WWW (non-standard port 8834)

Severity: Service

agentx (705/TCP)

Severity: Service

microsoft-ds (445/TCP)

Severity: Service

netbios-ns (137/UDP)

Severity: Service

sunrpc (111/TCP)

Severity: Service

tftp (69/UDP)

Severity: Service

5 Patch Details

The following sections provide details of missing patches detected on the network.

5.1 TWIKI:SecurityAlertExecuteCommandsWithRev

http://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithRev

Host name: 10.8.0.101
IP Address: 10.8.0.101
Host type: Windows Server 2003 SP2
Netbios name: WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki revision control shell command injection

Host name: 10.8.0.104
IP Address: 10.8.0.104
Host type: Windows XP SP3
Netbios name: XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki revision control shell command injection

Host name: 10.8.0.14
IP Address: 10.8.0.14
Host type: Windows XP SP2
Netbios name: XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki revision control shell command injection

Host name: 10.8.0.150
IP Address: 10.8.0.150
Host type: Windows Server 2008 R2
Netbios name: WIN-IQF3U12CJA5
Scan time: Dec 14 12:46:20 2015

- TWiki revision control shell command injection

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- TWiki revision control shell command injection

Host name: 10.8.0.230
IP Address: 10.8.0.230
Host type: Linux 3.13.0-57-generic - Ubuntu 14.04
Netbios name: UBUNTUNESSUS
Scan time: Dec 14 12:43:41 2015

- TWiki revision control shell command injection

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- TWiki revision control shell command injection

Host name: 10.8.0.46
IP Address: 10.8.0.46
Host type: Ubuntu 14.04
Netbios name: SAINT84VM64
Scan time: Dec 14 12:46:29 2015

- TWiki revision control shell command injection

5.2 TWIKI:SecurityAlertExecuteCommandsWithSearch

http://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithSearch

Host name: 10.8.0.101
IP Address: 10.8.0.101
Host type: Windows Server 2003 SP2
Netbios name: WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.104
IP Address: 10.8.0.104
Host type: Windows XP SP3
Netbios name: XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.14
IP Address: 10.8.0.14
Host type: Windows XP SP2
Netbios name: XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.150
IP Address: 10.8.0.150
Host type: Windows Server 2008 R2
Netbios name: WIN-IQF3U12CJA5
Scan time: Dec 14 12:46:20 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.230
IP Address: 10.8.0.230
Host type: Linux 3.13.0-57-generic - Ubuntu 14.04
Netbios name: UBUNTUNESSUS
Scan time: Dec 14 12:43:41 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- TWiki Search.pm shell command injection

Host name: 10.8.0.46
IP Address: 10.8.0.46
Host type: Ubuntu 14.04
Netbios name: SAINT84VM64
Scan time: Dec 14 12:46:29 2015

- TWiki Search.pm shell command injection

5.3 MS03-051

https://technet.microsoft.com/library/security/MS03-051

Host name: 10.8.0.101
Host type: Windows Server 2003 SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.101
Netbios name: WIN2003PATCHED

- FrontPage fp30reg.dll remote debug buffer overflow

Host name: 10.8.0.104
Host type: Windows XP SP3
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.104
Netbios name: XPSP3PATCHED

- FrontPage fp30reg.dll remote debug buffer overflow

Host name: 10.8.0.14
Host type: Windows XP SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.14
Netbios name: XPPROUNPATCHED

- FrontPage fp30reg.dll remote debug buffer overflow

Host name: 10.8.0.150
Host type: Windows Server 2008 R2
Scan time: Dec 14 12:46:20 2015
IP Address: 10.8.0.150
Netbios name: WIN-IQF3U12CJA5

- FrontPage fp30reg.dll remote debug buffer overflow

Host name: 10.8.0.20
Host type: Windows 8.1
Scan time: Dec 14 12:47:23 2015
IP Address: 10.8.0.20
Netbios name: WIN81

- FrontPage fp30reg.dll remote debug buffer overflow

Host name: 10.8.0.38
Host type: Windows 7 SP1
Scan time: Dec 14 12:47:24 2015
IP Address: 10.8.0.38
Netbios name: WIN7

- FrontPage fp30reg.dll remote debug buffer overflow

5.4 MS04-031

https://technet.microsoft.com/library/security/MS04-031

Host name: 10.8.0.101
Host type: Windows Server 2003 SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.101
Netbios name: WIN2003PATCHED

- Windows NetDDE buffer overflow

Host name: 10.8.0.104
Host type: Windows XP SP3
IP Address: 10.8.0.104
Netbios name: XPSP3PATCHED

Scan time: Dec 14 12:50:21 2015

- Windows NetDDE buffer overflow

Host name: 10.8.0.14
Host type: Windows XP SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.14
Netbios name: XPPROUNPATCHED

- Windows NetDDE buffer overflow

Host name: 10.8.0.150
Host type: Windows Server 2008 R2
Scan time: Dec 14 12:46:20 2015
IP Address: 10.8.0.150
Netbios name: WIN-IQF3U12CJA5

- Windows NetDDE buffer overflow

Host name: 10.8.0.20
Host type: Windows 8.1
Scan time: Dec 14 12:47:23 2015
IP Address: 10.8.0.20
Netbios name: WIN81

- Windows NetDDE buffer overflow

Host name: 10.8.0.38
Host type: Windows 7 SP1
Scan time: Dec 14 12:47:24 2015
IP Address: 10.8.0.38
Netbios name: WIN7

- Windows NetDDE buffer overflow

5.5 ORACLE:cpujuly2013-1899826

http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html

Host name: 10.8.0.101
Host type: Windows Server 2003 SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.101
Netbios name: WIN2003PATCHED

- Oracle Endeca Server createDataStore method command execution

Host name: 10.8.0.104
Host type: Windows XP SP3
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.104
Netbios name: XPSP3PATCHED

- Oracle Endeca Server createDataStore method command execution

Host name: 10.8.0.14
Host type: Windows XP SP2
Scan time: Dec 14 12:50:21 2015
IP Address: 10.8.0.14
Netbios name: XPPROUNPATCHED

- Oracle Endeca Server createDataStore method command execution

Host name: 10.8.0.150
Host type: Windows Server 2008 R2
Scan time: Dec 14 12:46:20 2015
IP Address: 10.8.0.150
Netbios name: WIN-IQF3U12CJA5

- Oracle Endeca Server createDataStore method command execution

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- Oracle Endeca Server createDataStore method command execution

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- Oracle Endeca Server createDataStore method command execution

5.6 VMWARE:VMSA-2011-0003

http://www.vmware.com/security/advisories/VMSA-2011-0003.html

Host name: 10.8.0.101
IP Address: 10.8.0.101
Host type: Windows Server 2003 SP2
Netbios name: WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015

- HP Performance Manager Apache Tomcat Policy Bypass

Host name: 10.8.0.104
IP Address: 10.8.0.104
Host type: Windows XP SP3
Netbios name: XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015

- HP Performance Manager Apache Tomcat Policy Bypass

Host name: 10.8.0.14
IP Address: 10.8.0.14
Host type: Windows XP SP2
Netbios name: XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015

- HP Performance Manager Apache Tomcat Policy Bypass

Host name: 10.8.0.150
IP Address: 10.8.0.150
Host type: Windows Server 2008 R2
Netbios name: WIN-IQF3U12CJA5
Scan time: Dec 14 12:46:20 2015

- HP Performance Manager Apache Tomcat Policy Bypass

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- HP Performance Manager Apache Tomcat Policy Bypass

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- HP Performance Manager Apache Tomcat Policy Bypass

5.7 MS05-039

https://technet.microsoft.com/library/security/MS05-039

Host name: 10.8.0.104 **Host type:** Windows XP SP3 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.104 **Netbios name:** XPSP3PATCHED

- Windows Plug and Play buffer overflow

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- Windows Plug and Play buffer overflow

Host name: 10.8.0.150 **Host type:** Windows Server 2008 R2 **Scan time:** Dec 14 12:46:20 2015	**IP Address:** 10.8.0.150 **Netbios name:** WIN-IQF3U12CJA5

- Windows Plug and Play buffer overflow

Host name: 10.8.0.20 **Host type:** Windows 8.1 **Scan time:** Dec 14 12:47:23 2015	**IP Address:** 10.8.0.20 **Netbios name:** WIN81

- Windows Plug and Play buffer overflow

Host name: 10.8.0.38 **Host type:** Windows 7 SP1 **Scan time:** Dec 14 12:47:24 2015	**IP Address:** 10.8.0.38 **Netbios name:** WIN7

- Windows Plug and Play buffer overflow

5.8 MS06-070

https://technet.microsoft.com/library/security/MS06-070

Host name: 10.8.0.101 **Host type:** Windows Server 2003 SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.101 **Netbios name:** WIN2003PATCHED

- Windows Workstation service NetpManageIPCConnect buffer overflow

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- Windows Workstation service NetpManageIPCConnect buffer overflow

Host name: 10.8.0.150
IP Address: 10.8.0.150
Host type: Windows Server 2008 R2
Netbios name: WIN-IQF3U12CJA5
Scan time: Dec 14 12:46:20 2015

- Windows Workstation service NetpManageIPCConnect buffer overflow

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- Windows Workstation service NetpManageIPCConnect buffer overflow

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- Windows Workstation service NetpManageIPCConnect buffer overflow

5.9 WIRESHARK:wnpa-sec-2011-06

http://www.wireshark.org/security/wnpa-sec-2011-06.html

Host name: 10.8.0.104
IP Address: 10.8.0.104
Host type: Windows XP SP3
Netbios name: XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015

- Wireshark DECT Dissector Remote Stack Buffer Overflow

Host name: 10.8.0.14
IP Address: 10.8.0.14
Host type: Windows XP SP2
Netbios name: XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015

- Wireshark DECT Dissector Remote Stack Buffer Overflow

Host name: 10.8.0.150
IP Address: 10.8.0.150
Host type: Windows Server 2008 R2
Netbios name: WIN-IQF3U12CJA5
Scan time: Dec 14 12:46:20 2015

- Wireshark DECT Dissector Remote Stack Buffer Overflow

Host name: 10.8.0.20
IP Address: 10.8.0.20
Host type: Windows 8.1
Netbios name: WIN81
Scan time: Dec 14 12:47:23 2015

- Wireshark DECT Dissector Remote Stack Buffer Overflow

Host name: 10.8.0.38
IP Address: 10.8.0.38
Host type: Windows 7 SP1
Netbios name: WIN7
Scan time: Dec 14 12:47:24 2015

- Wireshark DECT Dissector Remote Stack Buffer Overflow

5.10 MS00-078

https://technet.microsoft.com/library/security/MS00-078

Host name: 10.8.0.104 **Host type:** Windows XP SP3 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.104 **Netbios name:** XPSP3PATCHED

- IIS Unicode Directory Traversal

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- IIS Unicode Directory Traversal

Host name: 10.8.0.150 **Host type:** Windows Server 2008 R2 **Scan time:** Dec 14 12:46:20 2015	**IP Address:** 10.8.0.150 **Netbios name:** WIN-IQF3U12CJA5

- IIS Unicode Directory Traversal

5.11 MS01-026

https://technet.microsoft.com/library/security/MS01-026

Host name: 10.8.0.104 **Host type:** Windows XP SP3 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.104 **Netbios name:** XPSP3PATCHED

- IIS Double Decoding Directory Traversal

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- IIS Double Decoding Directory Traversal

Host name: 10.8.0.150 **Host type:** Windows Server 2008 R2 **Scan time:** Dec 14 12:46:20 2015	**IP Address:** 10.8.0.150 **Netbios name:** WIN-IQF3U12CJA5

- IIS Double Decoding Directory Traversal

5.12 MS08-067

https://technet.microsoft.com/library/security/MS08-067

Host name: 10.8.0.101 **Host type:** Windows Server 2003 SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.101 **Netbios name:** WIN2003PATCHED

- Windows Server Service buffer overflow MS08-067

Host name: 10.8.0.104 **Host type:** Windows XP SP3 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.104 **Netbios name:** XPSP3PATCHED

- Windows Server Service buffer overflow MS08-067

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- Windows Server Service buffer overflow MS08-067

5.13 ORACLE:cpuoct2008-100299

http://www.oracle.com/technetwork/topics/security/cpuoct2008-100299.html

Host name: 10.8.0.104 **Host type:** Windows XP SP3 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.104 **Netbios name:** XPSP3PATCHED

- Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

Host name: 10.8.0.14 **Host type:** Windows XP SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.14 **Netbios name:** XPPROUNPATCHED

- Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

Host name: 10.8.0.150 **Host type:** Windows Server 2008 R2 **Scan time:** Dec 14 12:46:20 2015	**IP Address:** 10.8.0.150 **Netbios name:** WIN-IQF3U12CJA5

- Oracle WebLogic Server Apache Connector Transfer-Encoding buffer overflow

5.14 MS03-026

https://technet.microsoft.com/library/security/MS03-026

Host name: 10.8.0.101 **Host type:** Windows Server 2003 SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.101 **Netbios name:** WIN2003PATCHED

- Windows RPC DCOM interface buffer overflow

Host name: 10.8.0.104	**IP Address:** 10.8.0.104
Host type: Windows XP SP3	**Netbios name:** XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows RPC DCOM interface buffer overflow

5.15 MS04-011

https://technet.microsoft.com/library/security/MS04-011

Host name: 10.8.0.104	**IP Address:** 10.8.0.104
Host type: Windows XP SP3	**Netbios name:** XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows LSASS buffer overflow

Host name: 10.8.0.14	**IP Address:** 10.8.0.14
Host type: Windows XP SP2	**Netbios name:** XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows LSASS buffer overflow

5.16 SNORT:advisory-2007-02-19

http://www.snort.org/docs/advisory-2007-02-19.html

Host name: 10.8.0.14	**IP Address:** 10.8.0.14
Host type: Windows XP SP2	**Netbios name:** XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015	

- Snort DCE/RPC preprocessor buffer overflow

Host name: 10.8.0.230	**IP Address:** 10.8.0.230
Host type: Linux 3.13.0-57-generic - Ubuntu 14.04	**Netbios name:** UBUNTUNESSUS
Scan time: Dec 14 12:43:41 2015	

- Snort DCE/RPC preprocessor buffer overflow

5.17 USN-2362-1

http://www.ubuntu.com/usn/USN-2362-1/

Host name: 10.8.0.230	**IP Address:** 10.8.0.230
Host type: Linux 3.13.0-57-generic - Ubuntu 14.04	**Netbios name:** UBUNTUNESSUS
Scan time: Dec 14 12:43:41 2015	

- Bash environment variable code injection over HTTP

Host name: 10.8.0.46 **Host type:** Ubuntu 14.04 **Scan time:** Dec 14 12:46:29 2015	**IP Address:** 10.8.0.46 **Netbios name:** SAINT84VM64

- Bash environment variable code injection over HTTP

5.18 USN-285-1

http://www.ubuntu.com/usn/USN-285-1/

Host name: 10.8.0.230 **Host type:** Linux 3.13.0-57-generic - Ubuntu 14.04 **Scan time:** Dec 14 12:43:41 2015	**IP Address:** 10.8.0.230 **Netbios name:** UBUNTUNESSUS

- AWStats migrate parameter command injection

Host name: 10.8.0.46 **Host type:** Ubuntu 14.04 **Scan time:** Dec 14 12:46:29 2015	**IP Address:** 10.8.0.46 **Netbios name:** SAINT84VM64

- AWStats migrate parameter command injection

5.19 USN-795-1

http://www.ubuntu.com/usn/USN-795-1/

Host name: 10.8.0.230 **Host type:** Linux 3.13.0-57-generic - Ubuntu 14.04 **Scan time:** Dec 14 12:43:41 2015	**IP Address:** 10.8.0.230 **Netbios name:** UBUNTUNESSUS

- Nagios statuswml.cgi Command Injection

Host name: 10.8.0.46 **Host type:** Ubuntu 14.04 **Scan time:** Dec 14 12:46:29 2015	**IP Address:** 10.8.0.46 **Netbios name:** SAINT84VM64

- Nagios statuswml.cgi Command Injection

5.20 CA:ca-alert-notification-server-multiple-vulnerabilities

http://community.ca.com/blogs/casecurityresponseblog/archive/2008/04/04
/ca-alert-notification-server-multiple-vulnerabilities.aspx

Host name: 10.8.0.101 **Host type:** Windows Server 2003 SP2 **Scan time:** Dec 14 12:50:21 2015	**IP Address:** 10.8.0.101 **Netbios name:** WIN2003PATCHED

- Computer Associates Alert Notification Server opcode 23 buffer overflow

5.21 MS06-025

https://technet.microsoft.com/library/security/MS06-025

Host name: 10.8.0.104	**IP Address:** 10.8.0.104
Host type: Windows XP SP3	**Netbios name:** XPSP3PATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows RRAS memory corruption vulnerability

5.22 MS06-040

https://technet.microsoft.com/library/security/MS06-040

Host name: 10.8.0.14	**IP Address:** 10.8.0.14
Host type: Windows XP SP2	**Netbios name:** XPPROUNPATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows Server Service buffer overflow

5.23 MS07-029

https://technet.microsoft.com/library/security/MS07-029

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Windows DNS server RPC management interface buffer overflow

5.24 ORACLE:2003Alert58

http://otn.oracle.com/deploy/security/pdf/2003Alert58.pdf

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle 9i Release 2 XDB HTTP Pass Overflow

5.25 ORACLE:2004alert68

http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle MD2 component SDO_CODE_SIZE buffer overflow

5.26 ORACLE:cpuapr2007-090632

http://www.oracle.com/technetwork/topics/security/cpuapr2007-090632.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle Database Advanced Replication component DBMS_SNAP_INTERNAL overflow

5.27 ORACLE:cpuapr2011-301950

http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle Warehouse Builder SQL Injection

5.28 ORACLE:cpujan2006-082403

http://www.oracle.com/technetwork/topics/security/cpujan2006-082403.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle XML Component DBMS_XMLSCHEMA.GENERATESCHEMA buffer overflow

5.29 ORACLE:cpujan2008-086860

http://www.oracle.com/technetwork/topics/security/cpujan2008-086860.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle XDB component PITRIG_TRUNCATE buffer overflow

5.30 ORACLE:cpujan2009-097901

http://www.oracle.com/technetwork/topics/security/cpujan2009-097901.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle Database OLAP component ODCITABLESTART buffer overflow

5.31 ORACLE:cpuoct2006-095368

http://www.oracle.com/technetwork/topics/security/cpuoct2006-095368.html

Host name: 10.8.0.101	**IP Address:** 10.8.0.101
Host type: Windows Server 2003 SP2	**Netbios name:** WIN2003PATCHED
Scan time: Dec 14 12:50:21 2015	

- Oracle Spatial component SDO_CS.TRANSFORM_LAYER buffer overflow

5.32 USN-460-1

http://www.ubuntu.com/usn/USN-460-1/

Host name: 10.8.0.230	**IP Address:** 10.8.0.230
Host type: Linux 3.13.0-57-generic - Ubuntu 14.04	**Netbios name:** UBUNTUNESSUS
Scan time: Dec 14 12:43:41 2015	

- Samba lsa_io_trans_names buffer overflow