SAINT® Vulnerability Assessment Report

SOX Vulnerability Assessment Report

Report Generated: March 19, 2013

1.0 Background

The Sarbanes-Oxley Act (SOX) holds corporate executives accountable for the information reported on key financial statements, and has made it mandatory for organizations to ensure their financial information is accurate, and systems generating the information are secure and reliable. This means developing policies and practices that ensure proper access controls, implementing effective patch management of financial systems and related architecture, and conducting vulnerability assessments and remediation activities to continuously monitor risk to target systems and content.

2.0 Introduction

On March 19, 2013, at 9:27 AM, a SOX vulnerability assessment was conducted using the SAINT 7.15.6 vulnerability scanner. The results in the Summary section below document the findings from this scan, to include details about the host, vulnerabilities found, and Common Vulnerability Scoring System (CVSS) numerical score. This scan discovered a total of three live hosts and detected four critical problems, nine areas of concern and 43 potential problems. The Summary and Details sections provide comprehensive information related to the vulnerabilities - to include content to assess risk and determine remediation.

This vulnerability scan and assessment where executed to support the organization.s overall internal risk management practices, as well as facilitate provisions in Section 404 of the Sarbanes-Oxley Act, requiring management report annually on the effectiveness of internal controls for financial reporting and that external auditors confirm management's assessment.

3.0 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN
Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

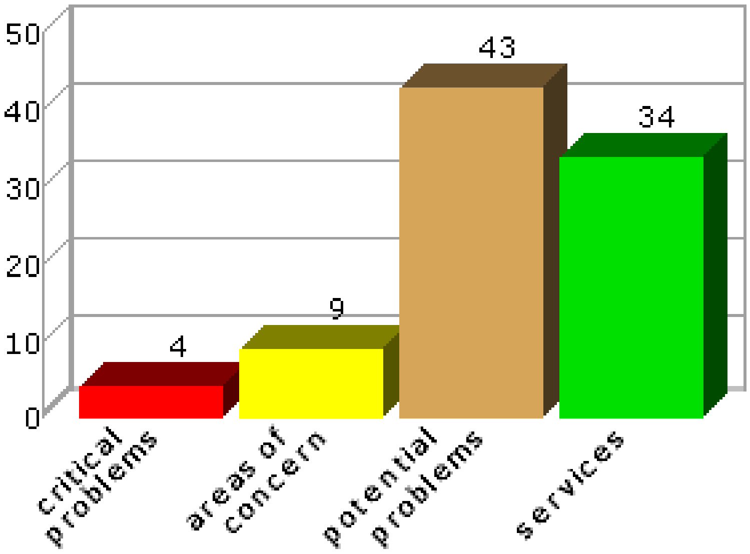
SERVICES

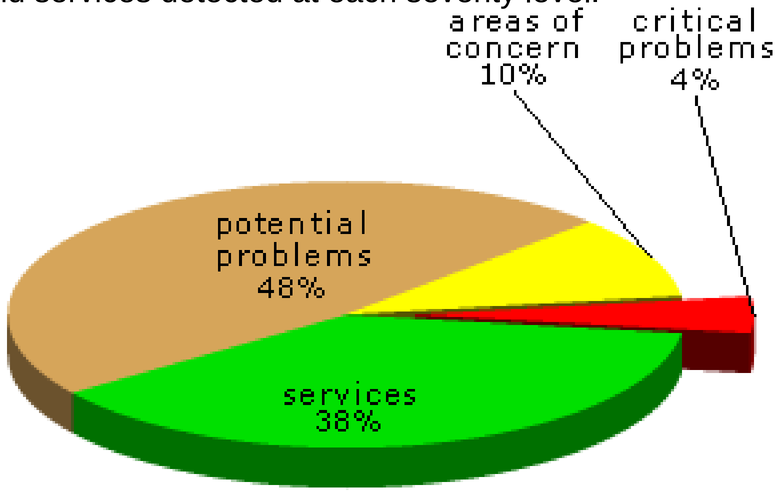
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

3.1 Vulnerabilities by Severity

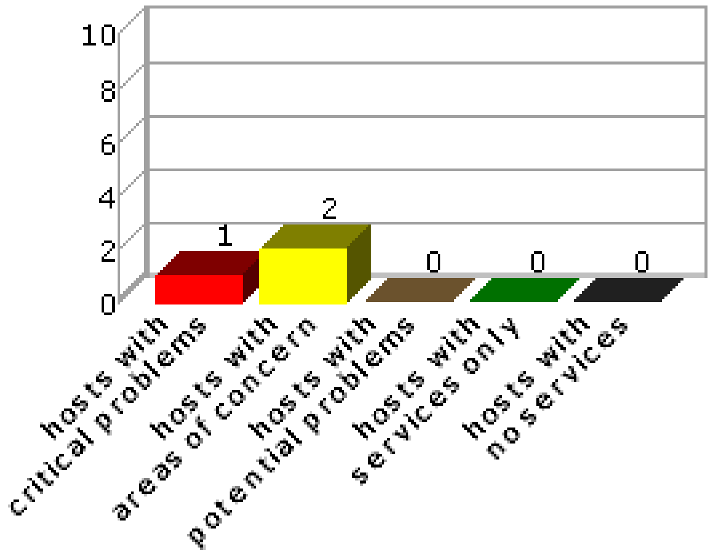
This section shows the overall number of vulnerabilities and services detected at each severity level.

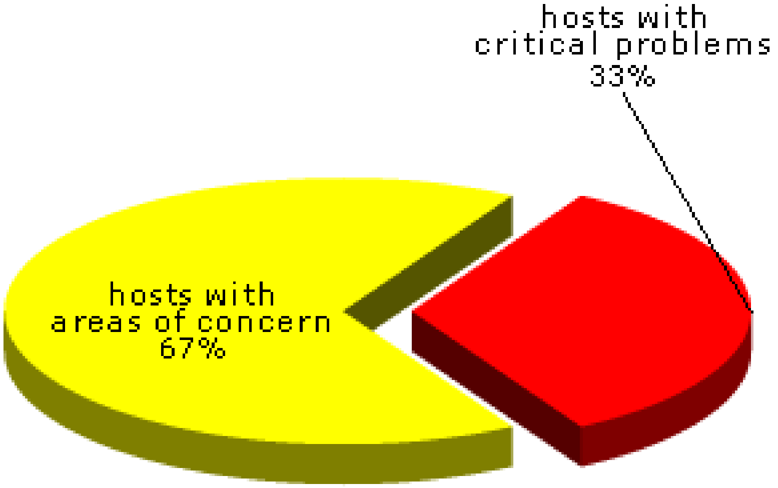




3.2 Hosts by Severity

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

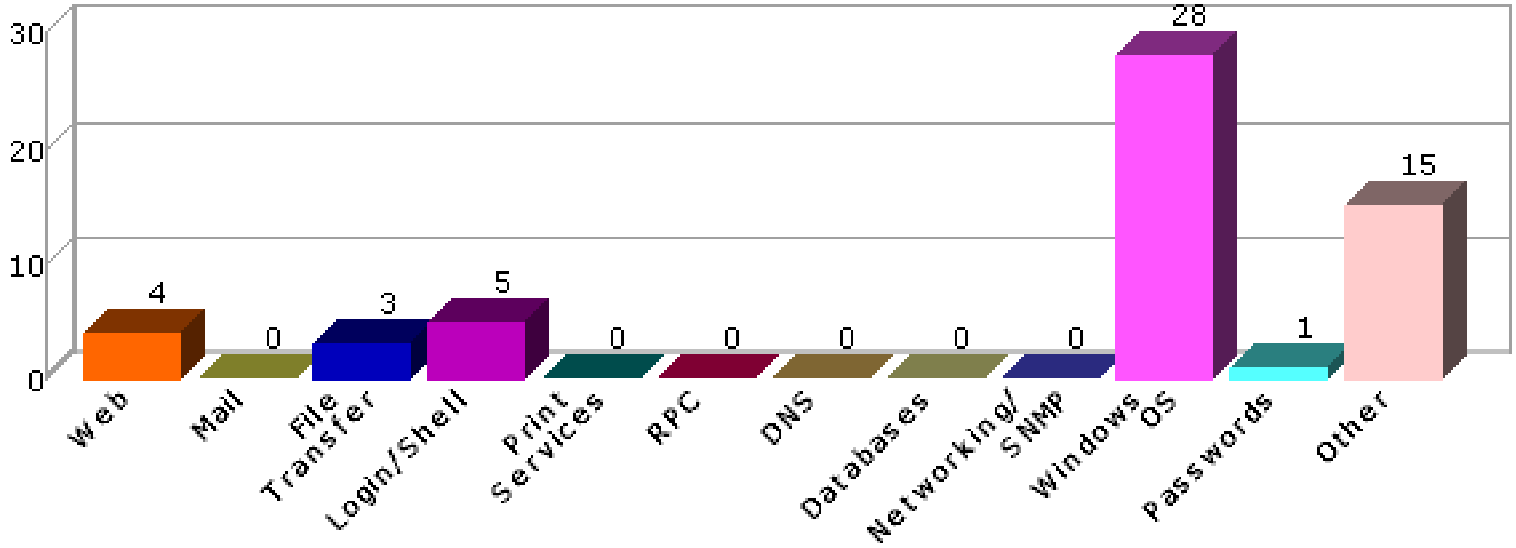


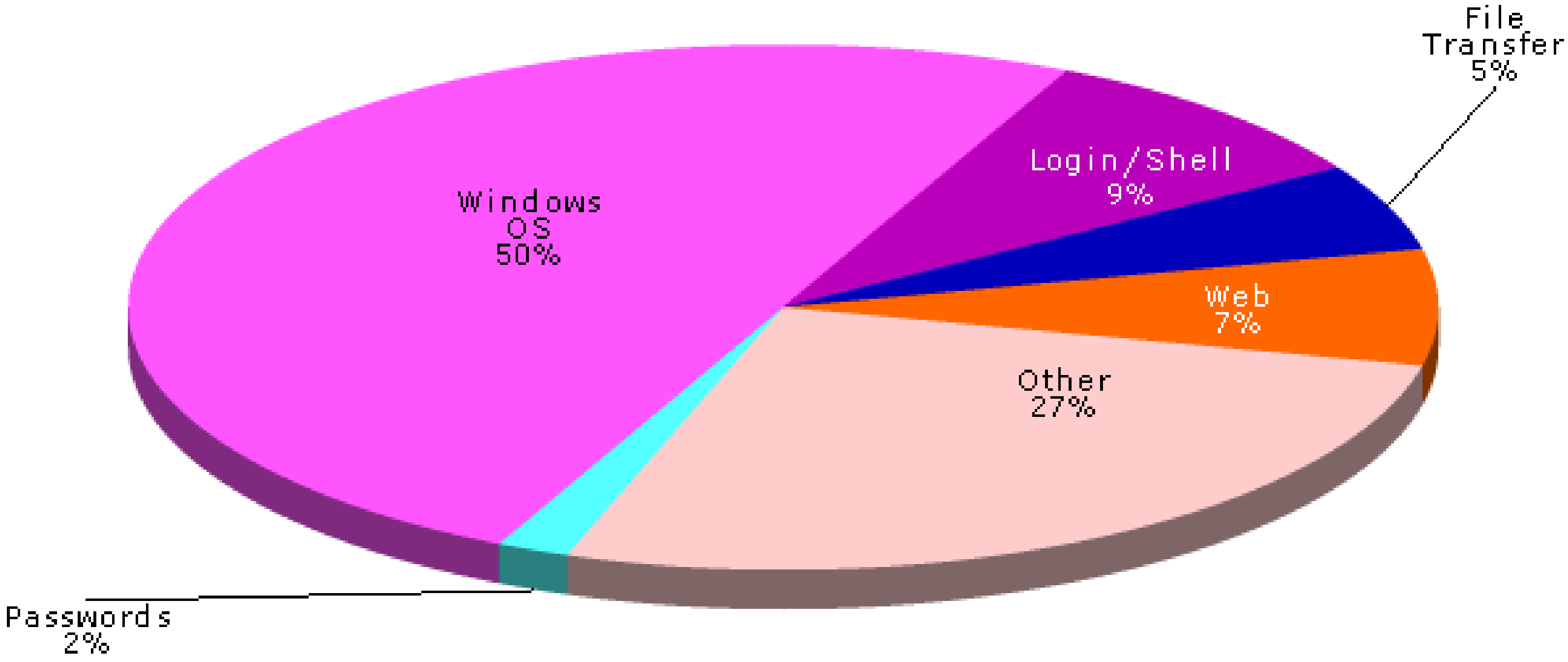


3.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each of the following classes.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes





4.0 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

4.1 Host List

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

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
freebsd		10.7.0.4	FreeBSD 4.11-RELEASE	4	3	9
10.7.0.101	WIN2003PATCHED	10.7.0.101	Windows Server 2003 SP2	0	5	27
10.7.0.176		10.7.0.176		0	1	7

4.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Max. CVSSv2 Base Score	Exploit Available?
freebsd	critical	vulnerability in FreeBSD telnetd	Login/Shell	CVE-2011-4862	10.0	yes
freebsd	critical	Guessed password to account (root:password)	Passwords	CVE-1999-0501 CVE-2006-5288	10.0	no
freebsd	critical	OpenSSH 3.5p1 is vulnerable	Login/Shell	CVE-2003-0190 CVE-2003-0386 CVE-2003-0682 CVE-2003-0693 CVE-2003-0695 CVE-2003-1562 CVE-2004-2069 CVE-2005-2797 CVE-2005-2798 CVE-2006-0225 CVE-2006-4924 CVE-2006-4925 CVE-2006-5051 CVE-2006-5052 CVE-2007-4752 CVE-2008-1483 CVE-2008-1657 CVE-2008-3259 CVE-2008-5161	10.0	no
freebsd	critical	possibly vulnerable tcpdump version: 3.7.2	Other	CVE-2007-1218 CVE-2007-3798	6.8	no
freebsd	concern	bzip2 vulnerable version: 1.0.2	Other	CVE-2010-0405	5.1	no
freebsd	concern	vulnerable GNU tar version: 1.13.25	Other	CVE-2006-0300 CVE-2006-6097 CVE-2007-4131 CVE-2007-4476	7.5	no

freebsd	concern	vulnerable gzip version: 1.2.4	Other	CVE-2006-4334 CVE-2006-4335 CVE-2006-4336 CVE-2006-4337 CVE-2006-4338 CVE-2009-2624 CVE-2010-0001	7.5	no
freebsd	potential	Possible globbing vulnerability in FreeBSD ftpd	File Transfer	CVE-2001-0247	10.0	no
freebsd	potential	FTP server does not support AUTH	File Transfer		2.6	no
freebsd	potential	ftp receives cleartext password	File Transfer		2.6	no
freebsd	potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0	no
freebsd	potential	Remote OS available	Other		2.6	no
freebsd	potential	SSH Protocol Version 1 Supported	Login/Shell	CVE-2001-0361 CVE-2001-1473	7.5	no
freebsd	potential	TCP timestamp requests enabled	Other		2.6	no
freebsd	potential	telnet receives cleartext passwords	Login/Shell		2.6	no
freebsd	potential	possible buffer overflow in telnetd telrcv	Login/Shell	CVE-2001-0554	10.0	no
freebsd	service	DNS				no
freebsd	service	FTP				no
freebsd	service	SSH				no
freebsd	service	Telnet				no
freebsd	service	XDM (X login)				no
freebsd	service	h323gatedisc (1718/UDP)				no
freebsd	service	h323gatestat (1719/UDP)				no
freebsd	service	syslog (514/UDP)				no
freebsd	service	tftp (69/UDP)				no
freebsd	info	User: bin				no
freebsd	info	User: bind				no
freebsd	info	User: daemon				no
freebsd	info	User: games				no
freebsd	info	User: gillmanj				no
freebsd	info	User: kline				no
freebsd	info	User: kmem				no
freebsd	info	User: mailnull				no
freebsd	info	User: man				no
freebsd	info	User: news				no
freebsd	info	User: nobody				no
freebsd	info	User: operator				no
freebsd	info	User: pop				no
freebsd	info	User: root				no
freebsd	info	User: smmsp				no
freebsd	info	User: sshd				no
freebsd	info	User: toor				no
freebsd	info	User: tty				no
freebsd	info	User: uucp				no
freebsd	info	User: www				no
freebsd	info	User: xten				no

10.7.0.101	concern	Internet Explorer 8 vulnerable version, mshtml.dll dated 2013-1-8	Windows OS	CVE-2013-0087 CVE-2013-0088 CVE-2013-0089 CVE-2013-0090 CVE-2013-0091 CVE-2013-0092 CVE-2013-0093 CVE-2013-0094 CVE-2013-1288	9.3	no
10.7.0.101	concern	Internet Explorer VBScript and JScript memory reallocation vulnerability (MS11-031)	Windows OS	CVE-2011-0663	9.3	no
10.7.0.101	concern	Jscript.dll buffer overflow vulnerability	Windows OS	CVE-2009-1920	9.3	no
10.7.0.101	concern	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (MS13-027)	Windows OS	CVE-2013-1285 CVE-2013-1286 CVE-2013-1287	7.2	no
10.7.0.101	concern	Windows VB script vulnerable version, vbscript.dll dated 2009-3-8	Windows OS	CVE-2010-0483 CVE-2011-0031	7.6	no
10.7.0.101	potential	AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)	Other		2.6	no
10.7.0.101	potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0	no
10.7.0.101	potential	ICMP redirects are allowed	Other		2.6	no
10.7.0.101	potential	Internet Explorer Shell.Explorer object enabled	Windows OS		2.6	no
10.7.0.101	potential	last user name shown in login box	Windows OS	CVE-1999-0592	10.0	no
10.7.0.101	potential	SMB digital signing is disabled	Windows OS		2.6	no
10.7.0.101	potential	password complexity policy disabled	Windows OS	CVE-1999-0535	10.0	no
10.7.0.101	potential	weak account lockout policy (0)	Windows OS	CVE-1999-0582	5.0	no
10.7.0.101	potential	weak minimum password age policy (0 days)	Windows OS	CVE-1999-0535	10.0	no
10.7.0.101	potential	weak minimum password length policy (0)	Windows OS	CVE-1999-0535	10.0	no
10.7.0.101	potential	weak password history policy (0)	Windows OS	CVE-1999-0535	10.0	no
10.7.0.101	potential	non-administrative users can bypass traverse checking	Windows OS	CVE-1999-0534	4.6	no
10.7.0.101	potential	non-administrative users can replace a process level token	Windows OS	CVE-1999-0534	4.6	no
10.7.0.101	potential	account management auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	account management failure auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	logon failure auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	object access auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	object access failure auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	policy change auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	policy change failure auditing disabled	Windows OS	CVE-1999-0575	7.5	no

10.7.0.101	potential	system event auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	system event failure auditing disabled	Windows OS	CVE-1999-0575	7.5	no
10.7.0.101	potential	Windows administrator account not renamed	Windows OS	CVE-1999-0585	2.1	no
10.7.0.101	potential	Windows guest account not renamed	Windows OS		0.9	no
10.7.0.101	potential	Windows TCP/IP Stack not hardened	Other		2.6	no
10.7.0.101	potential	Microsoft Windows Insecure Library Loading vulnerability	Windows OS		2.6	no
10.7.0.101	potential	Microsoft Windows Service Isolation Bypass Local Privilege Escalation	Windows OS	CVE-2010-1886	6.8	no
10.7.0.101	service	1029/TCP				no
10.7.0.101	service	DNS				no
10.7.0.101	service	SMB				no
10.7.0.101	service	XDM (X login)				no
10.7.0.101	service	epmap (135/TCP)				no
10.7.0.101	service	h323gatedisc (1718/UDP)				no
10.7.0.101	service	h323gatestat (1719/UDP)				no
10.7.0.101	service	isakmp (500/UDP)				no
10.7.0.101	service	microsoft-ds (445/TCP)				no
10.7.0.101	service	microsoft-ds (445/UDP)				no
10.7.0.101	service	ms-wbt-server (3389/TCP)				no
10.7.0.101	service	netbios-dgm (138/UDP)				no
10.7.0.101	service	netbios-ns (137/UDP)				no
10.7.0.101	service	ntp (123/UDP)				no
10.7.0.101	service	tftp (69/UDP)				no
10.7.0.101	info	OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Server 2003 R2 5.2]				no
10.7.0.101	info	User: Administrator (500)				no
10.7.0.101	info	User: Guest (501) (disabled)				no
10.7.0.101	info	User: HelpServicesGroup (1000)				no
10.7.0.101	info	User: SUPPORT_388945a0 (1001) (disabled)				no
10.7.0.101	info	User: TelnetClients (1002)				no
10.7.0.101	info	Windows service: Application Experience Lookup Service				no
10.7.0.101	info	Windows service: Application Layer Gateway Service				no
10.7.0.101	info	Windows service: Automatic Updates				no
10.7.0.101	info	Windows service: COM+ Event System				no
10.7.0.101	info	Windows service: COM+ System Application				no
10.7.0.101	info	Windows service: Computer Browser				no
10.7.0.101	info	Windows service: Cryptographic Services				no
10.7.0.101	info	Windows service: DCOM Server Process Launcher				no
10.7.0.101	info	Windows service: DHCP Client				no
10.7.0.101	info	Windows service: DNS Client				no

10.7.0.101	info	Windows service: Distributed Link Tracking Client	no
10.7.0.101	info	Windows service: Distributed Transaction Coordinator	no
10.7.0.101	info	Windows service: Error Reporting Service	no
10.7.0.101	info	Windows service: Event Log	no
10.7.0.101	info	Windows service: Help and Support	no
10.7.0.101	info	Windows service: IPSEC Services	no
10.7.0.101	info	Windows service: Logical Disk Manager	no
10.7.0.101	info	Windows service: Net Logon	no
10.7.0.101	info	Windows service: Network Connections	no
10.7.0.101	info	Windows service: Network Location Awareness (NLA)	no
10.7.0.101	info	Windows service: Plug and Play	no
10.7.0.101	info	Windows service: Print Spooler	no
10.7.0.101	info	Windows service: Protected Storage	no
10.7.0.101	info	Windows service: Remote Procedure Call (RPC)	no
10.7.0.101	info	Windows service: Remote Registry	no
10.7.0.101	info	Windows service: Secondary Logon	no
10.7.0.101	info	Windows service: Security Accounts Manager	no
10.7.0.101	info	Windows service: Server	no
10.7.0.101	info	Windows service: Shell Hardware Detection	no
10.7.0.101	info	Windows service: System Event Notification	no
10.7.0.101	info	Windows service: TCP/IP NetBIOS Helper	no
10.7.0.101	info	Windows service: Task Scheduler	no
10.7.0.101	info	Windows service: Terminal Services	no
10.7.0.101	info	Windows service: VMware Physical Disk Helper Service	no
10.7.0.101	info	Windows service: VMware Tools Service	no
10.7.0.101	info	Windows service: VMware Upgrade Helper	no
10.7.0.101	info	Windows service: Windows Audio	no
10.7.0.101	info	Windows service: Windows Firewall /Internet Connection Sharing (ICS)	no
10.7.0.101	info	Windows service: Windows Management Instrumentation	no
10.7.0.101	info	Windows service: Windows Time	no
10.7.0.101	info	Windows service: Wireless Configuration	no
10.7.0.101	info	Windows service: Workstation	no
10.7.0.101	info	lockout duration = 30m, reset = 30m, threshold = 0	no

10.7.0.176	concern	vulnerable Apache version: 2.2.16	Web	CVE-2010-1623 CVE-2011-0419 CVE-2011-1928 CVE-2011-3192 CVE-2011-3348 CVE-2011-3607 CVE-2011-4415 CVE-2012-0031 CVE-2012-0053 CVE-2012-3499 CVE-2012-4558	7.8	no
10.7.0.176	potential	Apache ETag header discloses inode numbers	Web	CVE-2003-1418	4.3	no
10.7.0.176	potential	web server autoindex enabled	Web	CVE-1999-0569	10.0	no
10.7.0.176	potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0	no
10.7.0.176	potential	Remote OS available	Other		2.6	no
10.7.0.176	potential	TCP reset using approximate sequence number	Other	CVE-2004-0230	5.0	no
10.7.0.176	potential	TCP timestamp requests enabled	Other		2.6	no
10.7.0.176	potential	Web server default page detected	Web		2.6	no
10.7.0.176	service	5280/TCP				no
10.7.0.176	service	6667/TCP				no
10.7.0.176	service	DNS				no
10.7.0.176	service	SSH				no
10.7.0.176	service	WWW				no
10.7.0.176	service	cbt (7777/TCP)				no
10.7.0.176	service	epmd (4369/TCP)				no
10.7.0.176	service	tftp (69/UDP)				no
10.7.0.176	service	xmpp-client (5222/TCP)				no
10.7.0.176	service	xmpp-server (5269/TCP)				no
10.7.0.176	info	Web Directory: /				no
10.7.0.176	info	Web Directory: /icons/				no
10.7.0.176	info	Web Directory: /icons/small/				no

5.0 Details

The following sections provide details on the specific vulnerabilities detected on each host.

5.1 freebsd

IP Address: 10.7.0.4 **Host type:** FreeBSD 4.11-RELEASE
Scan time: Mar 19 09:27:36 2013

vulnerability in FreeBSD telnetd

Severity: Critical Problem **CVE:** CVE-2011-4862

Impact

A remote attacker who can connect to the telnetd daemon could execute arbitrary commands with the privileges of the daemon which is usually the "root".

Resolution

- Upgrade your vulnerable system to security branch dated after the correction date, OR
- Apply the following patches to FreeBSD 7.4, 7.3, 8.2, and 8.1 systems. Download the patch from the location below, and verify the detached PGP signature using your PGP utility.
  - fetch telnetd.patch
  - fetch telnetd.patch.as

Where can I read more about this?

The `telnetd` Buffer Overflow vulnerability was reported in Secunia Advisory SA47397.

Technical Details

Service: telnet
Sent:
Long encryption key
Received:
AAA\x08\xff\xf0

Guessed password to account (root:password)

Severity: Critical Problem **CVE:** CVE-1999-0501 CVE-2006-5288

Impact

An attacker who is able to guess the password to a user account could gain shell access to the system with the privileges of the user. From there it is often trivial to gain complete control of 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. Enforce this policy using a utility such as npasswd in place of the default UNIX `passwd` program. Check the strength of all account passwords periodically using a password cracking utility such as Crack for Unix.

For Cisco 2700 Series Wireless Location Appliance, change the password or mitigate as described in cisco-air-20061013-wla.

Where can I read more about this?

Walter Belgers' paper, UNIX password security, is a good reference on strengthening passwords.

The Cisco 2700 Series WLA default password was described in cisco-sa-2006-1012-wla and Bugtraq ID 20490.

The IBM Totalstorage DS400 default password was posted to Full Disclosure.

Technical Details

Service: ssh
uid=0(root) gid=0(wheel) groups=0(wheel), 2(kmem), 3(sys), 4(tty), 5(operator), 20(staff), 31(guest)

OpenSSH 3.5p1 is vulnerable

Severity: Critical Problem		**CVE:**	CVE-2003-0190 CVE-2003-0386 CVE-2003-0682 CVE-2003-0693 CVE-2003-0695 CVE-2003-1562 CVE-2004-2069 CVE-2005-2797 CVE-2005-2798 CVE-2006-0225 CVE-2006-4924 CVE-2006-4925 CVE-2006-5051 CVE-2006-5052 CVE-2007-4752 CVE-2008-1483 CVE-2008-1657 CVE-2008-3259 CVE-2008-5161

Impact

This document describes some vulnerabilities in the OpenSSH cryptographic login program. Outdated versions of OpenSSH may allow a malicious user to log in as another user, to insert arbitrary commands into a session, or to gain remote root access to the OpenSSH server.

Resolution

Upgrade to OpenSSH version 5.8 or higher, or install a fix from your operating system vendor.

Where can I read more about this?

The CBC Mode Information Disclosure Vulnerability was announced by CPNI as Disclosure 3716 / CPNI-957037, with details documented in this advisory. Bugtraq ID 32319 includes an archived discussion and a page of references with links to vendors of various affected implementations of SSH. CERT posted Vulnerability Note VU#958563, which also has links to vendors' sites. The developers of OpenSSH summarize this issue on their security page with details and analysis in this advisory. Background information on the Cipher Block Chaining ("CBC") mode is available from NIST and Wikipedia.

The `X11UseLocalhost` X11 Forwarding Session Hijacking vulnerability was reported in Bugtraq ID 30339.

The `ForceCommand` Security Bypass was reported in Secunia Advisory SA29602.

The Forward X connections hijack was reported in Secunia Advisory SA29522.

The X11 Security Bypass was reported in Bugtraq ID 25628.

The vulnerabilities fixed by 4.4 were reported in OpenSSH 4.4 release.

The local SCP shell command execution vulnerability was reported in OpenSSH 4.3 release and Red Hat Bugzilla ID 168167.

The GatewayPorts and GSSAPI vulnerabilities were reported in the OpenSSH mailing list.

The LoginGraceTime denial of service was posted to openssh-unix-dev.

The PAM keyboard-interactive authentication weakness was reported in Bugtraq ID 7482.

The OpenSSH buffer management vulnerabilities are described in CERT Advisory 2003-24, Red Hat Security Advisory 2003:280, and a Bugtraq posting.

The Portable OpenSSH PAM vulnerabilities are described in the Portable OpenSSH Security Advisory, the

OpenPKG Security Advisory, and Bugtraq.

The reverse DNS lookup access control bypass was reported in Bugtraq.

Technical Details

Service: ssh

possibly vulnerable tcpdump version: 3.7.2

Severity: Critical Problem **CVE:** CVE-2007-1218 CVE-2007-3798

Impact

Vulnerabilities in tcpdump allow for remote code execution when processing a BGP packet.

Resolution

tcpdump should be upgraded to version 3.9.7 or higher or contact your vendor for an upgrade.

Where can I read more about this?

The `parse_elements` buffer overflow denial of service was reported in Secunia Advisory SA24318.

The BGP packet overflow remote code execution was reported in Bugtraq ID 24965.

Technical Details

Service: ssh
sent: tcpdump -V
received:
tcpdump version 3.7.2

bzip2 vulnerable version: 1.0.2

Severity: Area of Concern **CVE:** CVE-2010-0405

Impact

Vulnerability in BZIP2 could allow a remote attacker to execute arbitrary commands which may cause a denial of service.

Resolution

Upgrade to bzip2 1.0.6 or higher when available.

Where can I read more about this?

The Integer Overflow Vulnerability was reported in Bugtraq ID 43331.

Technical Details

Service: ssh
Sent:
bzip2 --help

Received:
bzip2, a block-sorting file compressor. Version 1.0.2, 30-Dec-2001.

vulnerable GNU tar version: 1.13.25

Severity: Area of Concern **CVE:** CVE-2006-0300 CVE-2006-6097 CVE-2007-4131 CVE-2007-4476

Impact

GNU Tar may be halted (denial of service) from a malformed TAR file. This vulnerability may also allow for the execution of arbitrary code. GNU Tar allows for directory traversal from a malformed TAR file.

Resolution

The slash slash dot dot directory traversal can be patched.

Upgrade to a version higher than GNU tar 1.16.

Where can I read more about this?

The `crashing stack` buffer overflow was reported in Secunia Advisory SA26674.

The GNU Tar slash slash dot dot directory traversal was reported in Bugtraq ID 25417.

The GNUTYPE_NAMES remote directory traversal vulnerability was reported in Bugtraq ID 21235.

The PAX extended header vulnerability was reported in Bugtraq ID 16764.

Technical Details

Service: ssh
sent: tar --version
received:
tar (GNU tar) 1.13.25

vulnerable gzip version: 1.2.4

Severity: Area of Concern **CVE:** CVE-2006-4334 CVE-2006-4335 CVE-2006-4336 CVE-2006-4337 CVE-2006-4338 CVE-2009-2624 CVE-2010-0001

Impact

Vulnerabilities in gzip allow for denial of service or execution of remote code when a file is decompacted using gunzip.

Resolution

Upgrade to a version of gzip higher than 1.3.12 when available.

Where can I read more about this?

The multiple vulnerabilities in gzip 1.3.12 and prior were reported in Bugtraq ID 37886, Bugtraq ID 37888.

The denial of service and remote code execution in 1.3.5 were reported in Secunia Advisory SA21996.

Technical Details

Service: ssh
sent: gzip -V
received:
gzip 1.2.4 (18 Aug 93)

Possible globbing vulnerability in FreeBSD ftpd

Severity: Potential Problem **CVE:** CVE-2001-0247

Impact

Regular users or anonymous users could gain root access on the server if this vulnerability is exploitable.

Resolution

For wu-ftpd, upgrade to wu-ftpd 2.6.2 or higher. This version fixes the problem described above, and also contains a fix for a format string vulnerability exposed when configured to use RFC 931 authentication and debug mode. (CVE 2001-0187)

For Linux servers other than wu-ftpd, install the latest version of the `glibc` package from your vendor. Although only the OpenBSD ftpd Linux port is known to be exploitable, it would be a good idea to upgrade `glibc` on all Linux systems, since there could be exploits discovered for other applications which depend on the glob function.

For other FTP servers, apply a patch or upgrade the FTP server. See CERT Advisory 2001-07 for instructions specific to your operating system. See CIRC Bulletin L-129 if your operating system is Solaris, CIRC Bulletin L-118 if your operating system is HP-UX, CIRC Bulletin L-135 if your operating system is IRIX, or Caldera Security Advisory 2001-SCO.27 if your operating system is UnixWare. If you are using glFTPd, upgrade to version 1.24.

Alternatively, disable the anonymous FTP account, or if that cannot be done, then:

1. ensure that there are no directories on the FTP server which are writable by the anonymous FTP account, and
2. ensure that there are no directories whose names are longer than eight characters

Note that this workaround only prevents the vulnerability from being exploited from the anonymous account. Exploitation would still be possible from a regular user account, resulting in privilege elevation.

Where can I read more about this?

For more information about the wu-ftpd vulnerability, see CERT Advisory 2001-33.

For more information about the `glibc` vulnerability, see Global InterSec advisory 2001121001 and CIRC Bulletin M-029.

For more information about the buffer overflow vulnerability, see CERT Advisory 2001-07 and the COVERT Labs Security Advisory.

The problem in glFTPd is a variation of the originally reported problem. See the posting to Bugtraq if you are using glFTPd.

Technical Details

Service: ftp
Received: 220 wwdsibsd FTP server (Version 6.00LS) ready.

FTP server does not support AUTH

Severity: Potential Problem

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the FTP server.

Resolution

Enable FTP Security Extensions on the FTP server. If the FTP server does not support Security Extensions, change to a different FTP server.

Where can I read more about this?

More information about FTP Security Extensions is available in RFC2228.

Technical Details

Service: ftp
Sent: AUTH SSL
Received: 500 'AUTH GSSAPI': command not understood.

ftp receives cleartext password

Severity: Potential Problem

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the FTP server.

Resolution

Disable the FTP server and use a more secure program such as SCP or SFTP to transfer files. If FTP cannot be disabled, restrict access using iptables or TCP Wrappers such that only addresses on a local, trusted network can connect.

Where can I read more about this?

For more information, see Protocols - The Problem With Cleartext.

Technical Details

Service: ftp
Received:
220 wwdsibsd FTP server (Version 6.00LS) ready.

```
500 'GET / HTTP/1.0': command not understood.
500 '': command not understood.
221 Goodbye.
```

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Impact

A remote attacker could obtain sensitive information about the network.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=02e60d86

Remote OS available

Severity: Potential Problem

Impact

The ability to detect which operating system is running on a machine enables attackers to be more accurate in attacks.

Resolution

Including the operating system in service banners is usually unnecessary. Therefore, change the banners of the services which are running on accessible ports. This can be done by disabling unneeded services, modifying the banner in a service's source code or configuration file if possible, or using TCP wrappers to modify the banner as described in the Red Hat Knowledgebase.

Where can I read more about this?

An example of ways to remove the Remote OS and other information is at my digital life.

Technical Details

Service: ssh
Received:
SSH-1.99-OpenSSH_3.5p1 FreeBSD-20030924

SSH Protocol Version 1 Supported

Severity: Potential Problem **CVE:** CVE-2001-0361 CVE-2001-1473

Impact

SSH protocol version 1 has a number of known vulnerabilities. Support for version 1 or enabling SSH1 Fallback renders the machines vulnerable to these issues.

Resolution

Disable SSH1 support and SSH1 fallback. See vendor website for more information including SSH, F-Secure and OpenSSH.

For OpenSSH servers, SSH1 support and SSH1 fallback can be disabled by placing the following line in the **`sshd_config`** file:

```
    Protocol 2
```

Where can I read more about this?

Some of the vulnerabilities in support for SSH Protocol 1 were reported in US-CERT Vulnerability Note VU#684820 and CIRC Bulletin M-017.

Technical Details

Service: ssh
Received:
22:ssh::SSH-1.99-OpenSSH_3.5p1 FreeBSD-20030924

TCP timestamp requests enabled

Severity: Potential Problem

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **`/etc/sysctl.conf`** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
Value: `Tcp1323Opts`
Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
no ip tcp timestamp
```

Where can I read more about this?

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: ftp
timestamp=203572743; uptime guess=23d 13h 28m 47s

telnet receives cleartext passwords

Severity: Potential Problem

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the telnet server.

Resolution

Disable the telnet service and use a more secure protocol such as SSH to access the computer remotely. If telnet cannot be disabled, restrict access using iptables or TCP Wrappers such that only addresses on a local, trusted network can connect.

Where can I read more about this?

For more information, see Protocols - The Problem With Cleartext.

Technical Details

Service: telnet
telnet service is enabled

possible buffer overflow in telnetd telrcv

Severity: Potential Problem **CVE:** CVE-2001-0554

Impact

Malicious users exploiting these vulnerabilities are able to gain unauthorized access or disrupt service on a target system.

Resolution

See CERT Advisory 2001-21 for information on obtaining patches for your particular operating system. See CIRC Bulletin L-128 if you are running the Kerberos version of telnetd. AIX users should see CIRC Bulletin L-131. IRIX users may refer to SGI Security Advisory 20010801-01-P. HP-UX users should see CIRC Bulletin M-006. Linux users should refer to the appropriate vendor advisory for patch information: Red Hat krb5 (Kerberos-telnetd), Red Hat telnetd, Caldera Linux telnetd, Debian telnetd, Debian telnetd-ssl, or Mandrake telnetd.

If a patch is not yet available, then TCP port 23 should be blocked at the network perimeter until a patch can be applied.

Where can I read more about this?

This vulnerability was reported in CIRC Bulletin L-124 and CERT Advisory 2001-21.

Technical Details

Service: telnet

DNS

Severity: Service

Technical Details

FTP

Severity: Service

Technical Details

```
220 wwdsibsd FTP server (Version 6.00LS) ready.
```

SSH

Severity: Service

Technical Details

```
SSH-1.99-OpenSSH_3.5p1 FreeBSD-20030924
```

Telnet

Severity: Service

Technical Details

\000

XDM (X login)

Severity: Service

Technical Details

h323gatedisc (1718/UDP)

Severity: Service

Technical Details

h323gatestat (1719/UDP)

Severity: Service

Technical Details

syslog (514/UDP)

Severity: Service

Technical Details

tftp (69/UDP)

Severity: Service

Technical Details

5.2 10.7.0.101

IP Address: 10.7.0.101	**Host type:** Windows Server 2003 SP2
Scan time: Mar 19 09:27:36 2013	**Netbios Name:** WIN2003PATCHED

Internet Explorer 8 vulnerable version, mshtml.dll dated 2013-1-8

Severity: Area of Concern

CVE: CVE-2013-0087 CVE-2013-0088
CVE-2013-0089 CVE-2013-0090
CVE-2013-0091 CVE-2013-0092
CVE-2013-0093 CVE-2013-0094
CVE-2013-1288

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 12-063, 12-071, 12-077, 13-008, 13-010, and 13-021.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
    Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
    Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, 11-081, 11-099, 12-010, 12-023, 12-037, 12-044, 12-052, 12-063, 12-071, 12-077, 13-008, 13-009, 13-010, and 13-021.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
mshtml.dll dated 2013-1-8, older than 2013-2-27

Internet Explorer VBScript and JScript memory reallocation vulnerability (MS11-031)

Severity: Area of Concern **CVE:** CVE-2011-0663

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 12-063, 12-071, 12-077, 13-008, 13-010, and 13-021.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, 11-081, 11-099, 12-010, 12-023, 12-037, 12-044, 12-052, 12-063, 12-071, 12-077, 13-008, 13-009, 13-010, and 13-021.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
jscript.dll dated 2009-3-8, older than 2011-2-14

Jscript.dll buffer overflow vulnerability

Severity: Area of Concern **CVE:** CVE-2009-1920

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 12-063, 12-071, 12-077, 13-008, 13-010, and 13-021.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
```

Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type *dword*, radix *hex*)

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, 11-081, 11-099, 12-010, 12-023, 12-037, 12-044, 12-052, 12-063, 12-071, 12-077, 13-008, 13-009, 13-010, and 13-021.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
jscript.dll dated 2009-3-8, older than 2009-6-1

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (MS13-027)

Severity: Area of Concern	**CVE:** CVE-2013-1285 CVE-2013-1286 CVE-2013-1287

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin

Windows Kernel-Mode Drivers Elevation of Privilege vulnerabilities	Three privately reported vulnerabilities in Microsoft Windows kernel-mode drivers could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. (CVE 2013-1285 CVE 2013-1286 CVE 2013-1287)	**XP 32-bit:**KB2807986 **XP 64-bit:**KB2807986 **2003 32-bit:**KB2807986 **2003 64-bit:**KB2807986 **Vista 32-bit:**KB2807986 **Vista 64-bit:**KB2807986 **2008 32-bit:**KB2807986 **2008 64-bit:**KB2807986 **W7 32-bit:**KB2807986 **W7 64-bit:**KB2807986 **2008 R2:**KB2807986 **W8 32-bit:**KB2807986 **W8 64-bit:**KB2807986 **2012:**KB2807986	13-027

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
usb8023.sys dated 2007-2-17, older than 2013-2-10

Windows VB script vulnerable version, vbscript.dll dated 2009-3-8

Severity: Area of Concern **CVE:** CVE-2010-0483 CVE-2011-0031

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Windows VB script vulnerable	Fixes remote code execution vulnerability which exists due to the way VB Script interacts with help files in Internet Explorer. (CVE 2010-0483)	Apply the appropriate patch	10-022
JScript and VBScript information disclosure vulnerability	Fixes an information disclosure vulnerability due to a memory corruption error. (CVE 2011-0031)	**Win 7:** 2475792 (32-bit) 2475792 (64-bit) **2008 R2:** 2475792	11-009

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
vbscript.dll dated 2009-3-8, older than 2010-3-7

AV Information: AntiVirus software not found (AVG F-Secure Forefront McAfee Symantec TrendMicro)

Severity: Potential Problem

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see Virus Bulletin.

Technical Details

Service: netbios
SAINT currently checks for AVG, F-Secure, Forefront, McAfee, Symantec, and TrendMicro AV software; none were detected

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Impact

A remote attacker could obtain sensitive information about the network.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

pre> deny icmp any any 13 deny icmp any any 17

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=ed74dc02

ICMP redirects are allowed

Severity: Potential Problem

Impact

An attacker could change the routing of packets from the target such that transmitted data could potentially be monitored or modified.

Resolution

Disable ICMP redirects. On Windows, this is done by setting the following registry value:

Key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
Name: `EnableICMPRedirect`
Type: `REG_DWORD`
Data: `0`

To disable ICMP redirects on Linux, use the following commands:

```
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.all.secure_redirects=0
```

To make the above settings permanent, also set the following lines in the **`/etc/sysctl.conf`** file:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
```

Where can I read more about this?

For more information about ICMP redirects, see Ask Ubuntu and Windows Reference.

For more information on securing the Linux kernel, see Linux Kernel /etc/sysctl.conf Security Hardening.

Technical Details

Service: registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect = 1

Internet Explorer Shell.Explorer object enabled

Severity: Potential Problem

Impact

A remote attacker could execute arbitrary commands on a client system when the client browses to a malicious web site hosted by the attacker.

Resolution

To use Internet Explorer securely, take the following steps:

(The vulnerabilities in IE 8, Beta 1 have not yet been patched)

(The response splitting and smuggling related to setRequestHeader() has not yet been patched)

(The file focus stealing vulnerability has not yet been patched)

(The stack overflow vulnerability has not yet been patched.)

(The document.open spoofing vulnerability has not yet been patched.)

- Install the appropriate cumulative patch for your version of Internet Explorer as outlined in Microsoft Security Bulletins 07-009, 07-061, 08-022, 08-032, 08-052, 10-002, 11-031, 12-063, 12-071, 12-077, 13-008, 13-010, and 13-021.
- Fix the Security Zone Bypass vulnerability (CVE-2010-0255) as described in Microsoft Security Advisory (980088)
- Prevent WPAD proxy server interception as described in Microsoft Knowledge Base Article 934864
- Disable the Javaprxy.dll object
- Disable the ADODB.Stream object
- Disable the Shell.Explorer object

Instructions for disabling the ADODB.Stream object can be found in Microsoft Knowledge Base Article 870669.

To disable the Shell.Explorer object, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}
Compatibility Flags = 400 (type dword, radix hex)
```

To disable the Javaprxy.dll object, install the update referenced in Microsoft Security Bulletin 05-037.

Where can I read more about this?

For more information on all Internet Explorer security fixes, see the Internet Explorer Critical Updates page.

For more information on specific vulnerabilities, see Microsoft Security Bulletins 03-004, 03-015, 03-020, 03-032, 03-040, 03-048, 04-004, 04-025, 04-038, 04-040, 05-014, 05-020, 05-025, 05-037, 05-038, 05-052, 05-054, 06-004, 06-013, 06-021, 06-023, 06-042, 06-055, 06-067, 06-072, 07-004, 07-009, 07-016, 07-027, 07-033, 07-045, 07-050, 07-057, 07-061, 07-069, 08-010, 08-022, 08-023, 08-024, 08-031, 08-032, 08-045, 08-052, 08-058, 08-073, 08-078, 09-002, 09-014, 09-019, 09-034, 09-045, 09-054, 09-072, 10-002, 10-018, 10-035, 10-053, 10-071, 10-090, 11-003, 11-018, 11-031, 11-052, 11-050, 11-057, 11-081, 11-099, 12-010, 12-023, 12-037, 12-044, 12-052, 12-063, 12-071, 12-077, 13-008, 13-009, 13-010, and 13-021.

Also see CERT advisories CA-2003-22, TA04-033A, TA04-163A, TA04-212A, TA04-293A, TA04-315A, TA04-336A, TA05-165A, TA05-221A, and US-CERT Vulnerability Note VU#378604.

The IE 8, Beta 1 vulnerabilities were reported in Bugtraq ID 28580 and Bugtraq ID 28581.

Unfixed variants of the drag and drop vulnerability and the Shell.Explorer object were discussed in NTBugtraq and Full Disclosure.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Internet Explorer\ActiveX
Compatibility\{8856F961-340A-11D0-A96B-00C04FD705A2}\Compatibility Flags is not 0x400

last user name shown in login box

Severity: Potential Problem **CVE:** CVE-1999-0592

Impact

An attacker with physical access to the computer could determine a valid user name on the system, thus facilitating password guessing attacks.

Resolution

Run **`regedt32`**, and in the key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`, set `DontDisplayLastUserName` equal to `1`.

Where can I read more about this?

More information is available in The Registry Guide for Windows.

Technical Details

Service: netbios
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName = 0

SMB digital signing is disabled

Severity: Potential Problem

Impact

If the SMB signing is disabled, malicious attackers could sniff the network traffic and could perform a man in the middle attack to gain sensitive information.

Resolution

Refer to Microsoft Technet Library in Local Policies, Microsoft network server: Digitally sign communications (if client agrees).

Where can I read more about this?

For more information about SMB signing configuration, see, SMB Protocol Package Exchange Scenario.

Technical Details

Service: netbios
NEGOTIATE_SECURITY_SIGNATURES_ENABLED=0

password complexity policy disabled

Severity: Potential Problem **CVE:** CVE-1999-0535

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn

weak account lockout policy (0)

Severity: Potential Problem **CVE:** CVE-1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
0 > 3 or 0 = 0

weak minimum password age policy (0 days)

Severity: Potential Problem **CVE:** CVE-1999-0535

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn

0 < 2

weak minimum password length policy (0)

Severity: Potential Problem **CVE:** CVE-1999-0535

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
0 < 8

weak password history policy (0)

Severity: Potential Problem **CVE:** CVE-1999-0535

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days

- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
0 < 24

non-administrative users can bypass traverse checking

Severity: Potential Problem **CVE:** CVE-1999-0534

Impact

Normal users could take actions which should be limited to administrators. These privileges could be used to facilitate attacks or to make system resources unavailable to other users.

Resolution

Edit the user rights assignment, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's documentation on User Rights Assignment.

Technical Details

Service: netbios-ssn
SeChangeNotifyPrivilege

non-administrative users can replace a process level token

Severity: Potential Problem **CVE:** CVE-1999-0534

Impact

Normal users could take actions which should be limited to administrators. These privileges could be used to facilitate attacks or to make system resources unavailable to other users.

Resolution

Edit the user rights assignment, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's documentation on User Rights Assignment.

Technical Details

Service: netbios-ssn
SeAssignPrimaryTokenPrivilege

account management auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

account management failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

logon failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

object access auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

object access failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

policy change auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

policy change failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

system event auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

system event failure auditing disabled

Severity: Potential Problem **CVE:** CVE-1999-0575

Impact

Intrusion attempts or other unauthorized activities could go unnoticed.

Resolution

Edit the auditing policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's guide to setting up auditing and developing an auditing policy.

Technical Details

Service: netbios-ssn

Windows administrator account not renamed

Severity: Potential Problem **CVE:** CVE-1999-0585

Impact

The default administrator and guest account names give attackers a starting point for conducting brute-force password guessing attacks.

Resolution

Change the name of the administrator and guest accounts. To do this on Active Directory servers, open *Active Directory Users and Computers*. Click *Users*, then right-click on Administrator or Guest, and select *Rename*. To do this on workstations, open the *Local Security Policy* from the Administrative Tools menu. Choose *Local Policies*, then *Security Options*, then Accounts: Rename administrator or guest account.

Where can I read more about this?

For more information on securing the administrator account, see The Administrator Accounts Security Planning Guide - Chapter 3.

Technical Details

Service: netbios-ssn
UID 500 = Administrator

Windows guest account not renamed

Severity: Potential Problem

Impact

The default administrator and guest account names give attackers a starting point for conducting brute-force password guessing attacks.

Resolution

Change the name of the administrator and guest accounts. To do this on Active Directory servers, open *Active Directory Users and Computers*. Click *Users*, then right-click on Administrator or Guest, and select *Rename*. To do this on workstations, open the *Local Security Policy* from the Administrative Tools menu. Choose *Local Policies*, then *Security Options*, then Accounts: Rename administrator or guest account.

Where can I read more about this?

For more information on securing the administrator account, see The Administrator Accounts Security Planning

Guide - Chapter 3.

Technical Details

Service: netbios-ssn
UID 501 = Guest

Windows TCP/IP Stack not hardened

Severity: Potential Problem

Impact

A remote attacker could cause a temporary denial of service.

Resolution

Apply the TCP/IP stack hardening guidelines discussed in Microsoft Knowledge Base Article 324270 for Windows Server 2003 or 315669 for Windows XP. (Although the latter article was written for Windows 2000, it is presumably also effective for Windows XP.) The patch referenced in Microsoft Security Bulletin 05-019 also fixes this vulnerability, but not for IPv6 interfaces.

Where can I read more about this?

Land was originally reported in CERT Advisory 1997-28. The Land attack relating to Windows XP Service Pack 2 and Windows Server 2003 was posted to Bugtraq. The Land attack relating to IPv6 was posted to NTBugtraq.

Technical Details

Service: netbios
KB324270/315669 recommendations not applied for XP SP2 or 2003

Microsoft Windows Insecure Library Loading vulnerability

Severity: Potential Problem

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Windows Insecure Library Loading vulnerability	A remote attacker could execute DLL preloading attacks through an SMB share or WebDAV.	Disable loading of libraries from WebDAV and remote network shares as described in Microsoft KB 2264107.	2269637

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Technical Details

Service: netbios
SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch does not exist

Microsoft Windows Service Isolation Bypass Local Privilege Escalation

Severity: Potential Problem **CVE:** CVE-2010-1886

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Microsoft Windows Service Isolation Bypass Local Privilege Escalation	Fixed a vulnerability which leverages the Windows Service Isolation feature to gain elevation of privilege. (CVE 2010-1886)	**TAPI** 982316	2264072

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows 2000, Windows NT 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server

2008, and Windows 7.

Technical Details

Service: netbios
Tapisrv.dll dated 2007-2-17, older than 2010-4-22

1029/TCP

Severity: Service

Technical Details

DNS

Severity: Service

Technical Details

SMB

Severity: Service

Technical Details

\131\000\000\001\143

XDM (X login)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

h323gatedisc (1718/UDP)

Severity: Service

Technical Details

h323gatestat (1719/UDP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

microsoft-ds (445/UDP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

tftp (69/UDP)

Severity: Service

Technical Details

5.3 10.7.0.176

IP Address: 10.7.0.176
Scan time: Mar 19 09:27:36 2013

vulnerable Apache version: 2.2.16

Severity: Area of Concern

CVE: CVE-2010-1623 CVE-2011-0419 CVE-2011-1928 CVE-2011-3192 CVE-2011-3348 CVE-2011-3607 CVE-2011-4415 CVE-2012-0031 CVE-2012-0053 CVE-2012-3499 CVE-2012-4558

Impact

A remote attacker could crash the web server, disclose certain sensitive information, or execute arbitrary commands.

Resolutions

Upgrade Apache 2.0.x to a version higher than 2.0.64 when available, 2.2.x to 2.2.24 or higher. or a version higher than 2.4.3, or install an updated package from your Linux vendor.

Where can I read more about this?

The multiple Cross-Site Scripting vulnerabilities fixed in 2.2.24 were reported in Secunia Advisory SA52394.

The `"httpOnly"` Cookie Disclosure and Denial of Service vulnerabilities were reported in Secunia Advisory SA47779.

The Scoreboard Invalid Free Security Bypass vulnerability was reported in Secunia Advisory SA47410.

The `"ap_pregsub()"` Denial of Service vulnerability was reported in Secunia Advisory SA46823.

The `"ap_pregsub()"` Privilege Escalation vulnerability was reported in Secunia Advisory SA45793.

The `mod_proxy_ajp` Denial of Service vulnerability was reported in Secunia Advisory SA46013.

The `ByteRange` Filter Denial of Service vulnerability was reported in Secunia Advisory SA45606.

The `APR "apr_fnmatch()"` Infinite Loop Denial of Service vulnerability was reported in Secunia Advisory SA44661.

The `APR apr_fnmatch` Denial of Service vulnerability was reported in Secunia Advisory SA44574.

The `APR apr_brigade_split_line` Denial of Service vulnerability was reported in Bugtraq ID 43673.

The HTTP-Basic Authentication Bypass vulnerability was reported in Bugtraq ID 35840.

The Apache HTTP Server OS Fingerprinting Unspecified Security vulnerability was reported in Bugtraq ID 31805.

Technical Details

Service: http
Received: Server: Apache/2.2.16 (Debian)

Apache ETag header discloses inode numbers

Severity: Potential Problem **CVE:** CVE-2003-1418

Impact

A remote attacker could determine inode numbers on the server.

Resolution

Use the `FileETag` directive to remove the INode component from the calculation of the ETag. For example, place the following line in the Apache configuration file to calculate the ETag based only on the file's modification time and size:

```
FileETag MTime Size
```

Where can I read more about this?

This vulnerability was reported in Bugtraq ID 6939.

Technical Details

Service: http
Sent:
GET / HTTP/1.0
Host: 10.7.0.176
User-Agent: Mozilla/5.0
Received:
ETag: "10124-b1-4addc9a101c00"

web server autoindex enabled

Severity: Potential Problem **CVE:** CVE-1999-0569

Impact

A remote attacker could view the directory structure on the web server.

Resolutions

Ensure that autoindexing is not enabled on the web server. On Apache web servers, this can be done with the following directive in the configuration file:

```
Options -Indexes
```

Where can I read more about this?

For more information, see the Apache mod_autoindex documentation.

Technical Details

Service: http
Index of /icons/small
Index of /icons

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Impact

A remote attacker could obtain sensitive information about the network.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=02e62116

Remote OS available

Severity: Potential Problem

Impact

The ability to detect which operating system is running on a machine enables attackers to be more accurate in attacks.

Resolution

Including the operating system in service banners is usually unnecessary. Therefore, change the banners of the services which are running on accessible ports. This can be done by disabling unneeded services, modifying the banner in a service's source code or configuration file if possible, or using TCP wrappers to modify the banner as described in the Red Hat Knowledgebase.

Where can I read more about this?

An example of ways to remove the Remote OS and other information is at my digital life.

Technical Details

Service: http
Received:
Server: Apache/2.2.16 (Debian)

TCP reset using approximate sequence number

Severity: Potential Problem **CVE:** CVE-2004-0230

Impact

A remote attacker could cause a denial of service on systems which rely upon persistent TCP connections.

Resolution

To correct this problem on Cisco devices, apply one of the fixes referenced in the Cisco security advisories for IOS and non-IOS operating systems. Refer to US-CERT Vulnerability Note VU#415294 and NISSC vulnerability advisory 236929 for other vendor fixes.

If a fix is not available, this problem can be worked around by using a secure protocol such as IPsec, or by filtering incoming connections to services such as BGP which rely on persistent TCP connections at the firewall, such that only allowed addresses may reach them.

Where can I read more about this?

This vulnerability was reported in US-CERT alert 04-111A.

For more information on TCP, see RFC793.

Technical Details

Service: tcp
sent spoofed RST packet, received RST packet

TCP timestamp requests enabled

Severity: Potential Problem

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **`/etc/sysctl.conf`** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

> Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
> Value: `Tcp1323Opts`
> Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
   no ip tcp timestamp
```

Where can I read more about this?

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: cbt
timestamp=471252346; uptime guess=21d 21h 42m 59s

Web server default page detected

Severity: Potential Problem

Impact

An unconfigured web server creates an unnecessary security exposure on the network.

Resolution

Disable unconfigured web servers. If the web server is needed, replace the default page with some appropriate site-specific content.

Where can I read more about this?

For more information about default web pages, see about.com.

Technical Details

Service: http
Received:
<html><body><h1>It works!</h1>

5280/TCP

Severity: Service

Technical Details

6667/TCP

Severity: Service

Technical Details

:teal.saintcorporation.local NOTICE Auth :*** Looking up your hostname...

DNS

Severity: Service

Technical Details

SSH

Severity: Service

Technical Details

```
SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2
```

WWW

Severity: Service

Technical Details

```
HTTP/1.1 200 OK
Date: Tue, 19 Mar 2013 13:23:21 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Mon, 26 Sep 2011 18:48:16 GMT
ETag: "10124-b1-4addc9a101c00"
Accept-Ranges:
```

cbt (7777/TCP)

Severity: Service

Technical Details

epmd (4369/TCP)

Severity: Service

Technical Details

tftp (69/UDP)

Severity: Service

Technical Details

xmpp-client (5222/TCP)

Severity: Service

Technical Details

```
<?xml version='1.0'?><stream:stream xmlns='jabber:client' xmlns:stream='http://etherx.jabber.org/streams'
id='785717765' from='team' version='1.0'><stream:error><xml-not-well-formed
xmlns='urn:ietf:params:xml:ns:xmpp-streams'/></stream:error></stream:stream>
```

xmpp-server (5269/TCP)

Severity: Service

Technical Details

```
<?xml version='1.0'?><stream:stream xmlns:stream='http://etherx.jabber.org/streams' xmlns='jabber:server'
xmlns:db='jabber:server:dialback' id='1133283737'><stream:error><xml-not-well-formed
xmlns='urn:ietf:params:xml:ns:xmpp-streams'/></stream:error></stream:stream>
```

Scan Session: sox_dir; Scan Policy: SOX; Scan Data Set: 19 March 2013 09:27