Trend Report

Report Generated: December 15, 2015

1 Introduction

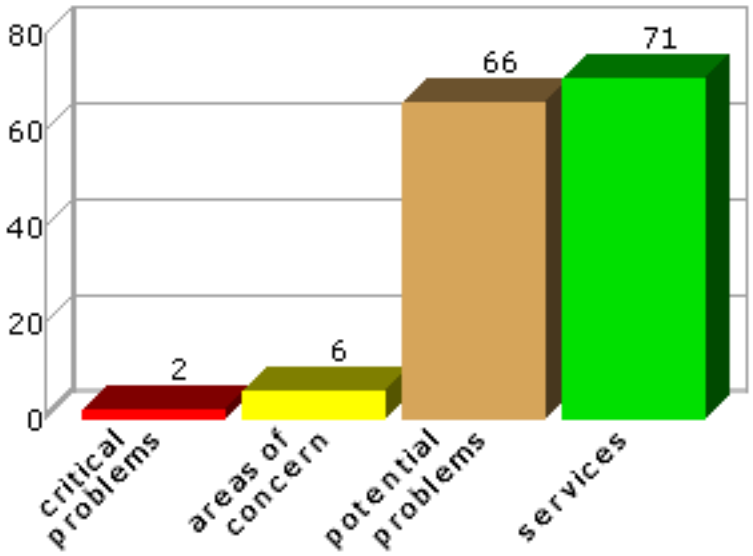
On December 15, 2015, at 6:10 AM, a heavy vulnerability assessment was conducted using the SAINT 8.9.28 vulnerability scanner. The scan discovered a total of six live hosts, and detected two critical problems, six areas of concern, and 66 potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

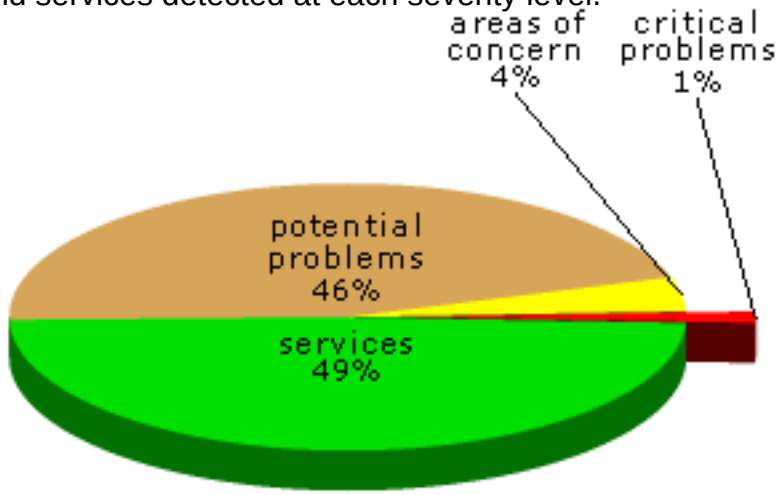
2 Summary

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

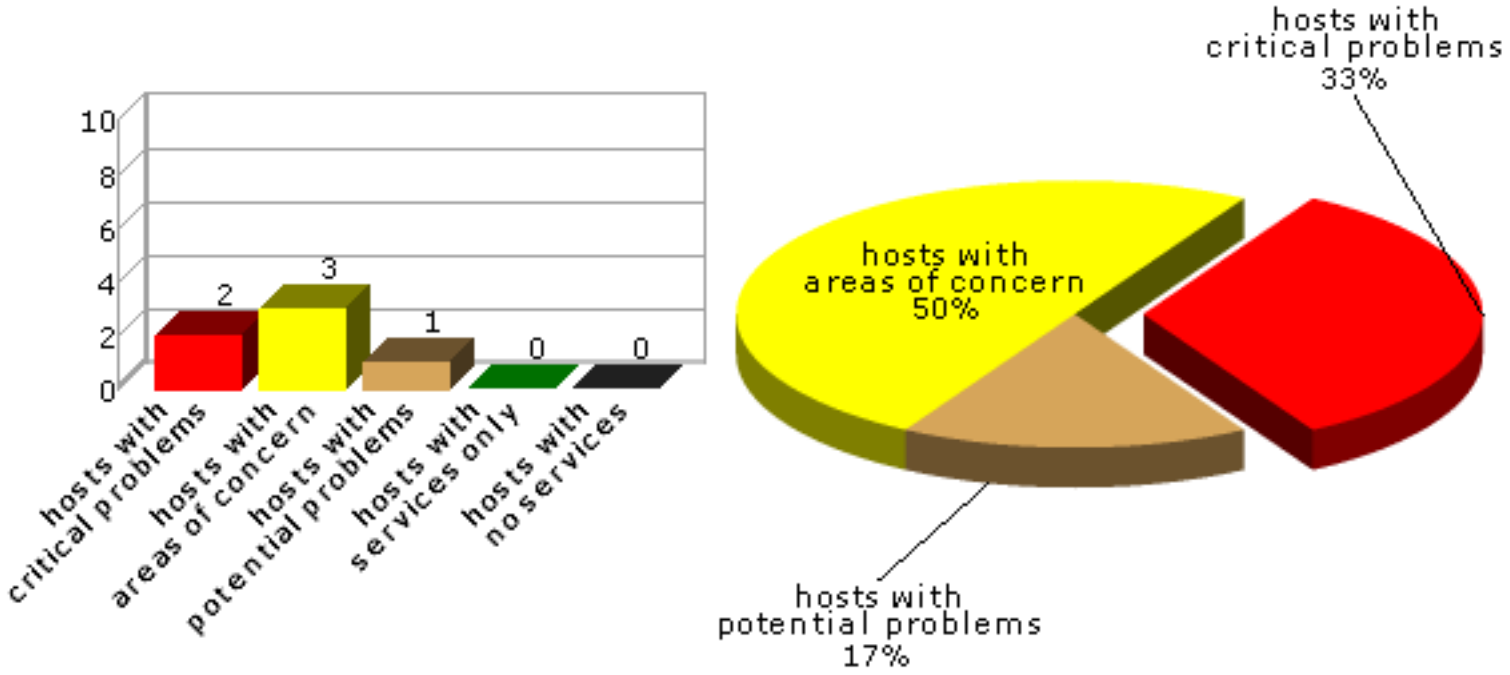
This section shows the overall number of vulnerabilities and services detected at each severity level.





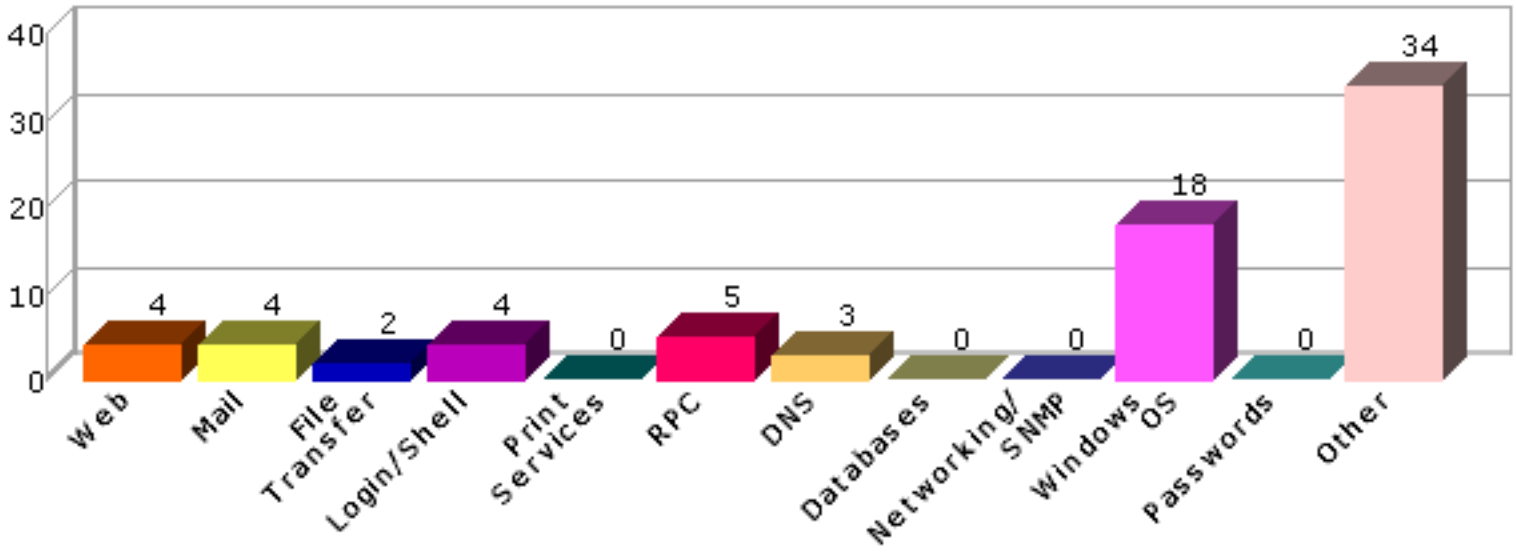
2.2 Hosts by Severity

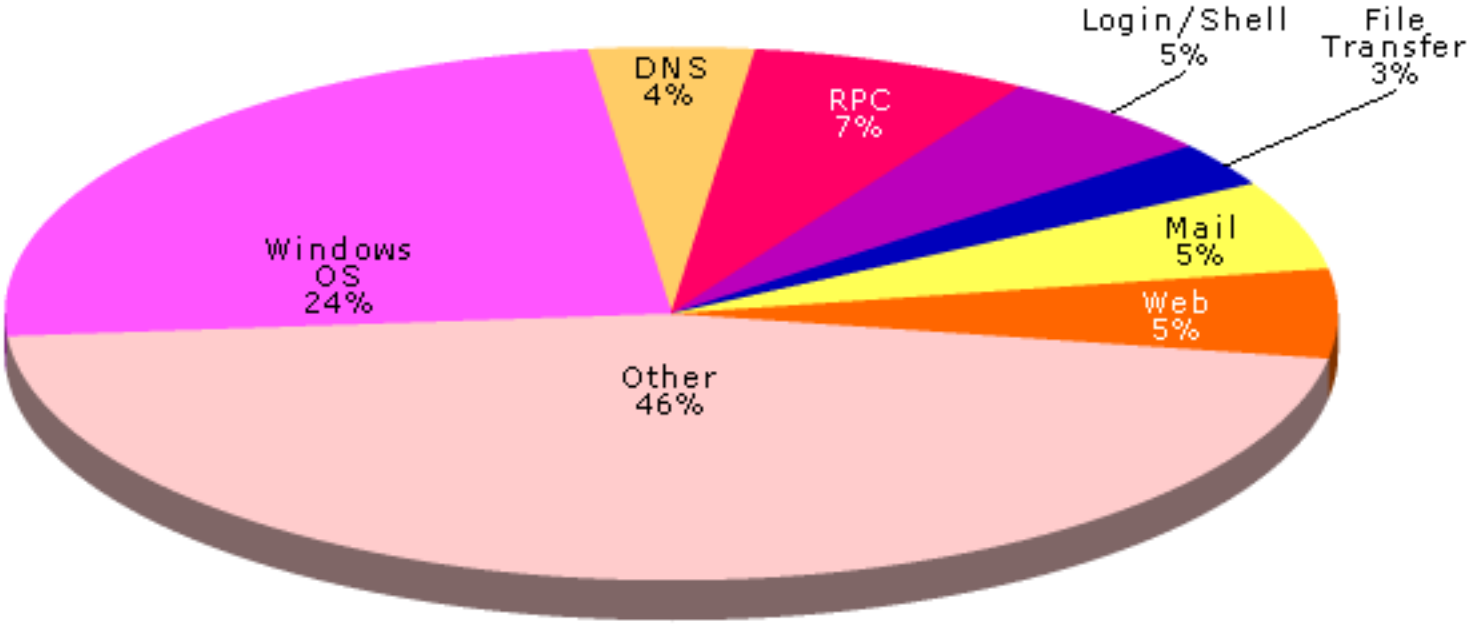
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.



2.3 Vulnerabilities by Class

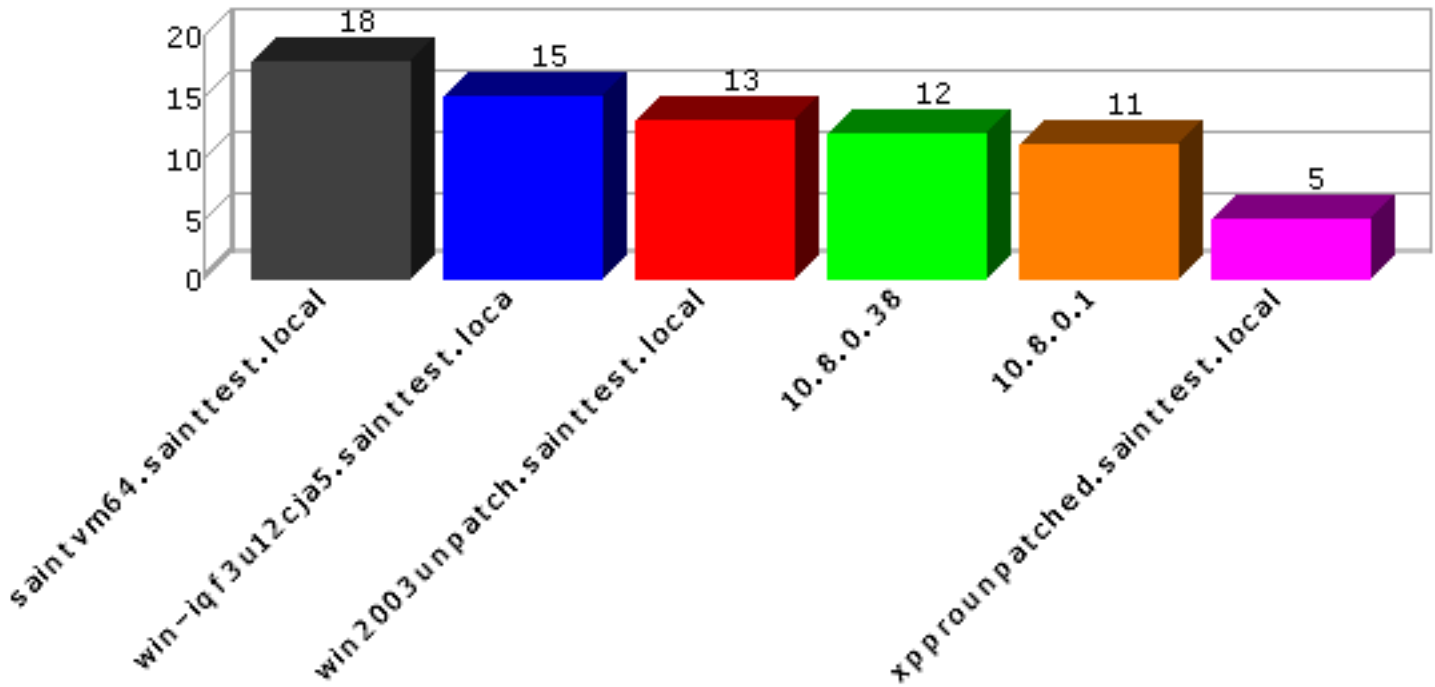
This section shows the number of vulnerabilities detected in each vulnerability class.





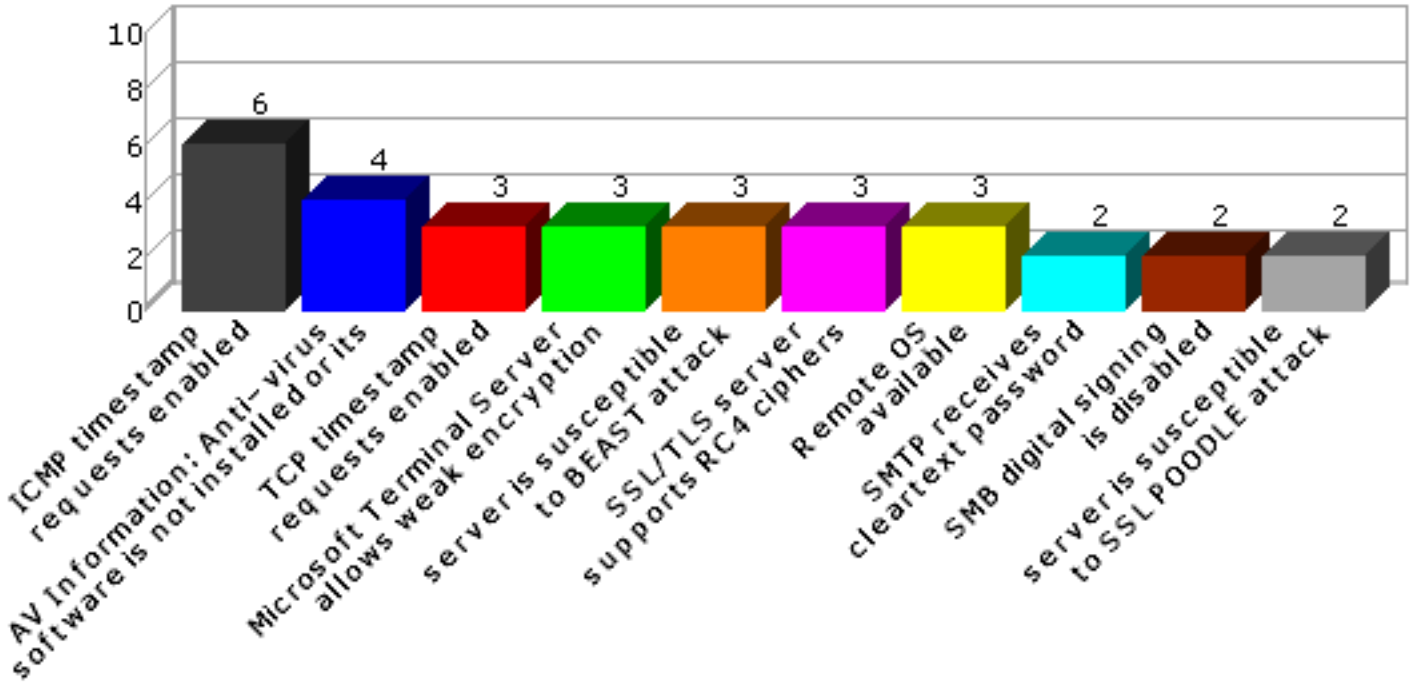
2.4 Top 10 Vulnerable Hosts

This section shows the most vulnerable hosts detected, and the number of vulnerabilities detected on them.



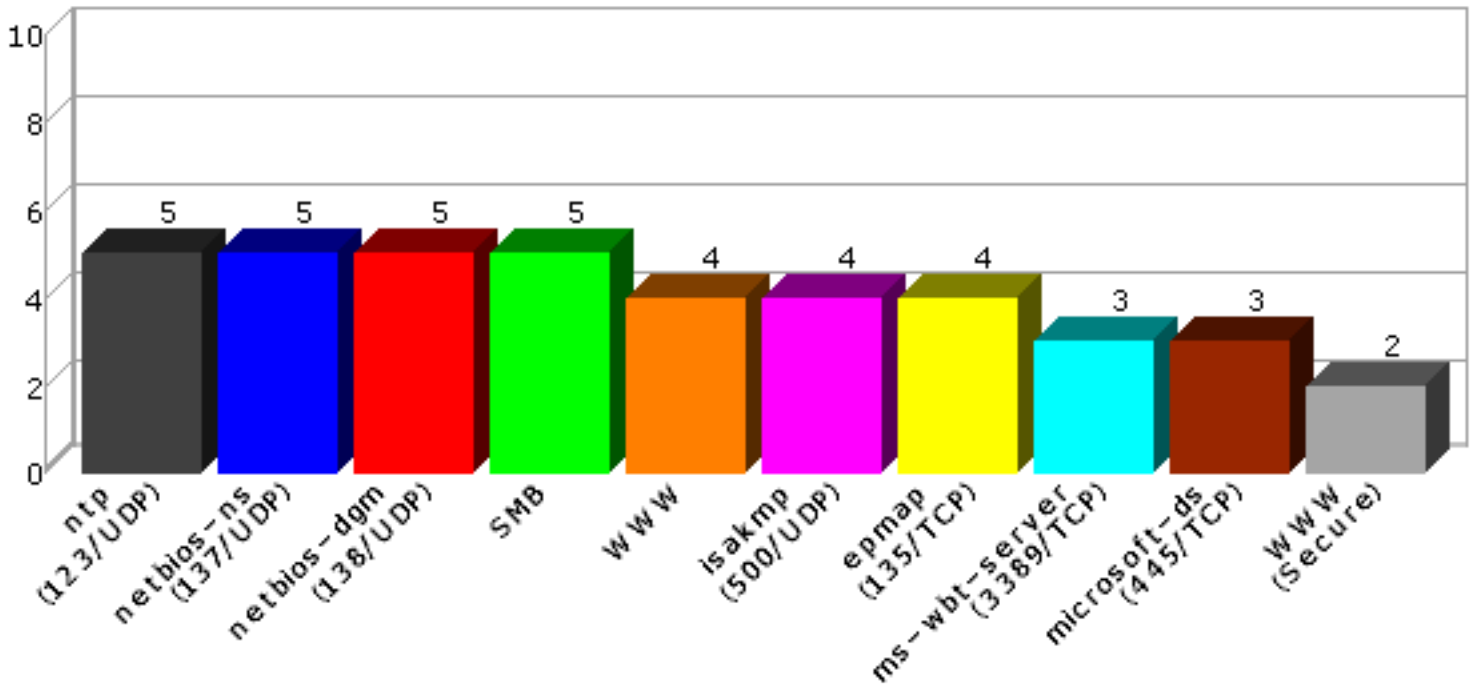
2.5 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, 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 vulnerabilities contained therein.

3.1 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
10.8.0.1		10.8.0.1	Cisco IOS 11.1	0	0	11
win2003unpatch.sainttest.local	WIN2003UNPATCH	10.8.0.11	Windows Server 2003	0	2	11
xpprounpatched.sainttest.local	XPPROUNPATCHED	10.8.0.14	Windows 2000	1	0	4
saintvm64.sainttest.local	SAINTVM64	10.8.0.35	Ubuntu 12.04	1	1	16
10.8.0.38	WIN7	10.8.0.38	Windows 7 SP1	0	1	11
win-iqf3u12cja5.sainttest.local	WIN-IQF3U12CJA5	10.8.0.150	Windows Server 2008 R2	0	2	13

3.2 Vulnerability List

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

Host Name	Port	Severity	Vulnerability / Service	Class	CVE	Max. CVSSv2 Base Score
10.8.0.1	443 /tcp	potential	server is susceptible to BEAST attack	Other	CVE-2011-3389	4.3
10.8.0.1		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
10.8.0.1	80/tcp	potential	Remote OS available	Other		2.6
10.8.0.1	22/tcp	potential	Remote OS available	Other		2.6
10.8.0.1	22/tcp	potential	SSH supports weak ciphers	Login /Shell		2.6
10.8.0.1	22/tcp	potential	SSH Protocol Version 1 Supported	Login /Shell	CVE-2001-0361 CVE-2001-1473	7.5
10.8.0.1	443 /tcp	potential	SSL certificate is self signed	Other		2.6
10.8.0.1	443 /tcp	potential	SSL server accepts weak ciphers	Other		2.6
10.8.0.1	443 /tcp	potential	server is susceptible to SSL POODLE attack	Other	CVE-2014-3566	4.3
10.8.0.1	443 /tcp	potential	SSL/TLS server supports RC4 ciphers	Other	CVE-2013-2566 CVE-2015-2808	4.3
10.8.0.1	23/tcp	potential	telnet receives cleartext passwords	Login /Shell		2.6
10.8.0.1	22/tcp	service	SSH			
10.8.0.1	23/tcp	service	Telnet			
10.8.0.1	80/tcp	service	WWW			
10.8.0.1	443 /tcp	service	WWW (Secure)			

10.8.0.1	1701 /udp	service	l2f (1701/UDP)			
win2003unpatch.sainttest.local	80/tcp	concern	vulnerable Microsoft.NET Framework version: 1.1.4322	Windows OS	CVE-2007-0041 CVE-2007-0042 CVE-2007-0043	9.3
win2003unpatch.sainttest.local	139 /tcp	concern	Group Policy Code Execution Vulnerability (MS15-011)	Windows OS	CVE-2015-0008	8.3
win2003unpatch.sainttest.local	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
win2003unpatch.sainttest.local	80/tcp	potential	Possible Microsoft IIS ASP Remote Code Execution vulnerability	Web	CVE-2008-0075	10.0
win2003unpatch.sainttest.local	80/tcp	potential	Possible Microsoft IIS ASP Upload Command Execution vulnerability	Web	CVE-2006-0026	6.5
win2003unpatch.sainttest.local	80/tcp	potential	web server allows MIME sniffing	Web		2.6
win2003unpatch.sainttest.local		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
win2003unpatch.sainttest.local	143 /tcp	potential	imap receives cleartext password	Mail		2.6
win2003unpatch.sainttest.local	139 /tcp	potential	Obsolete Windows Release: Windows Server 2003	Other		2.6
win2003unpatch.sainttest.local		potential	pop receives password in clear	Mail		2.6
win2003unpatch.sainttest.local	587 /tcp	potential	SMTP receives cleartext password	Mail		2.6
win2003unpatch.sainttest.local	25/tcp	potential	SMTP receives cleartext password	Mail		2.6
win2003unpatch.sainttest.local	80/tcp	potential	Web server default page detected	Web		2.6
win2003unpatch.sainttest.local	587 /tcp	service	587/TCP			
win2003unpatch.sainttest.local	1026 /udp	service	1026/UDP			
win2003unpatch.sainttest.local	1027 /udp	service	1027/UDP			
win2003unpatch.sainttest.local	143 /tcp	service	IMAP			
win2003unpatch.sainttest.local	110 /tcp	service	POP			
win2003unpatch.sainttest.local	139 /tcp	service	SMB			
win2003unpatch.sainttest.local	25/tcp	service	SMTP			
win2003unpatch.sainttest.local	80/tcp	service	WWW			
win2003unpatch.sainttest.local	135 /tcp	service	epmap (135/TCP)			
win2003unpatch.sainttest.local	500 /udp	service	isakmp (500/UDP)			
win2003unpatch.sainttest.local	138 /udp	service	netbios-dgm (138/UDP)			
win2003unpatch.sainttest.local	137 /udp	service	netbios-ns (137/UDP)			
win2003unpatch.sainttest.local	123 /udp	service	ntp (123/UDP)			

xpprounpatched.sainttest.local	3389	critical	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)	Windows OS	CVE-2012-0002 CVE-2012-0152	9.3
xpprounpatched.sainttest.local	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
xpprounpatched.sainttest.local		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
xpprounpatched.sainttest.local	3389 /tcp	potential	Possible vulnerability in Microsoft Terminal Server	Other	CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218	7.5
xpprounpatched.sainttest.local	3389	potential	Microsoft Terminal Server allows weak encryption	Other		2.6
xpprounpatched.sainttest.local	1026 /udp	service	1026/UDP			
xpprounpatched.sainttest.local	139 /tcp	service	SMB			
xpprounpatched.sainttest.local	80/tcp	service	WWW			
xpprounpatched.sainttest.local	1025 /udp	service	blackjack (1025/UDP)			
xpprounpatched.sainttest.local	135 /tcp	service	epmap (135/TCP)			
xpprounpatched.sainttest.local	500 /udp	service	isakmp (500/UDP)			
xpprounpatched.sainttest.local	3389 /tcp	service	ms-wbt-server (3389/TCP)			
xpprounpatched.sainttest.local	138 /udp	service	netbios-dgm (138/UDP)			
xpprounpatched.sainttest.local	137 /udp	service	netbios-ns (137/UDP)			
xpprounpatched.sainttest.local	123 /udp	service	ntp (123/UDP)			
xpprounpatched.sainttest.local	1900 /udp	service	ssdp (1900/UDP)			
saintvm64.sainttest.local	139 /tcp	critical	vulnerability in Samba 3.6.3	Windows OS	CVE-2012-1182 CVE-2012-2111 CVE-2013-0454 CVE-2013-4124 CVE-2013-4408 CVE-2013-4475 CVE-2013-4496 CVE-2014-0178 CVE-2014-0244 CVE-2014-3493 CVE-2014-8143 CVE-2015-0240	10.0
saintvm64.sainttest.local	22/tcp	concern	OpenSSH 5.9p1 is vulnerable	Login /Shell	CVE-2010-5107 CVE-2014-1692 CVE-2014-2532 CVE-2014-2653 CVE-2015-5352 CVE-2015-5600	8.5
saintvm64.sainttest.local		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
saintvm64.sainttest.local	139 /tcp	potential	NetBIOS share enumeration using null session	Windows OS		2.6

saintvm64.sainttest.local	139 /tcp	potential	Windows null session domain SID disclosure	Windows OS	CVE-2000-1200	5.0
saintvm64.sainttest.local	139 /tcp	potential	Windows null session host SID disclosure	Windows OS		2.6
saintvm64.sainttest.local	139 /tcp	potential	excessive null session access	Windows OS	CVE-2000-1200	5.0
saintvm64.sainttest.local	22/tcp	potential	Remote OS available	Other		2.6
saintvm64.sainttest.local	47152 /tcp	potential	rpc.statd is enabled and may be vulnerable	RPC	CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800	10.0
saintvm64.sainttest.local	139 /tcp	potential	SMB digital signing is disabled	Windows OS		2.6
saintvm64.sainttest.local	111 /tcp	potential	The sunrpc portmapper service is running	Other	CVE-1999-0632	0.0
saintvm64.sainttest.local	111 /tcp	potential	sunrpc services may be vulnerable	RPC	CVE-2002-0391 CVE-2003-0028	10.0
saintvm64.sainttest.local	111 /tcp	potential	TCP timestamp requests enabled	Other		2.6
saintvm64.sainttest.local	139 /tcp	potential	password complexity policy disabled	Windows OS	CVE-1999-0535	10.0
saintvm64.sainttest.local	139 /tcp	potential	weak account lockout policy (0)	Windows OS	CVE-1999-0582	5.0
saintvm64.sainttest.local	139 /tcp	potential	weak minimum password age policy (0 days)	Windows OS	CVE-1999-0535	10.0
saintvm64.sainttest.local	139 /tcp	potential	weak minimum password length policy (5)	Windows OS	CVE-1999-0535	10.0
saintvm64.sainttest.local	139 /tcp	potential	weak password history policy (0)	Windows OS	CVE-1999-0535	10.0
saintvm64.sainttest.local	139 /tcp	service	SMB			
saintvm64.sainttest.local	22/tcp	service	SSH			
saintvm64.sainttest.local	445 /tcp	service	microsoft-ds (445/TCP)			
saintvm64.sainttest.local	138 /udp	service	netbios-dgm (138/UDP)			
saintvm64.sainttest.local	137 /udp	service	netbios-ns (137/UDP)			
saintvm64.sainttest.local	123 /udp	service	ntp (123/UDP)			
saintvm64.sainttest.local	111 /tcp	service	sunrpc (111/TCP)			
saintvm64.sainttest.local	111 /udp	service	sunrpc (111/UDP)			
saintvm64.sainttest.local	139 /tcp	info	Netbios Attribute: Master Browser			
saintvm64.sainttest.local	139 /tcp	info	Netbios Attribute: Messenger Service			
saintvm64.sainttest.local	139 /tcp	info	OS=[Unix] Server=[Samba 3.6.3]			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-2 portmapper (111/TCP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-2 portmapper (111/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-3 portmapper (111/TCP)			

saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-3 portmapper (111/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-4 portmapper (111/TCP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100000-4 portmapper (111/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100007-1 ypbind (773/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100007-1 ypbind (775/TCP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100007-2 ypbind (773/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100007-2 ypbind (775/TCP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100024-1 status (34239/UDP)			
saintvm64.sainttest.local	111 /tcp	info	RPC service: 100024-1 status (47152/TCP)			
saintvm64.sainttest.local	139 /tcp	info	Share: print$			
saintvm64.sainttest.local	139 /tcp	info	User: nobody (501)			
saintvm64.sainttest.local	139 /tcp	info	lockout duration = 30m, reset = 30m, threshold = 0			
10.8.0.38	21/tcp	concern	vulnerable FileZilla server version: 0.9.41-beta	File Transfer	CVE-2014-0160 CVE-2014-0224	6.8
10.8.0.38	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
10.8.0.38	21/tcp	potential	server is susceptible to BEAST attack	Other	CVE-2011-3389	4.3
10.8.0.38	3389 /tcp	potential	server is susceptible to BEAST attack	Other	CVE-2011-3389	4.3
10.8.0.38	21/tcp	potential	ftp receives cleartext password	File Transfer		2.6
10.8.0.38		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
10.8.0.38	3389	potential	Microsoft Terminal Server allows weak encryption	Other		2.6
10.8.0.38	139 /tcp	potential	SMB digital signing is disabled	Windows OS		2.6
10.8.0.38	21/tcp	potential	server is susceptible to SSL POODLE attack	Other	CVE-2014-3566	4.3
10.8.0.38	3389 /tcp	potential	SSL/TLS server supports RC4 ciphers	Other	CVE-2013-2566 CVE-2015-2808	4.3
10.8.0.38	21/tcp	potential	SSL/TLS server supports RC4 ciphers	Other	CVE-2013-2566 CVE-2015-2808	4.3
10.8.0.38	139 /tcp	potential	TCP timestamp requests enabled	Other		2.6
10.8.0.38	21/tcp	service	FTP			
10.8.0.38	139 /tcp	service	SMB			
10.8.0.38	135 /tcp	service	epmap (135/TCP)			
10.8.0.38	500 /udp	service	isakmp (500/UDP)			
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	138 /udp	service	netbios-dgm (138/UDP)			
10.8.0.38	137 /udp	service	netbios-ns (137/UDP)			
10.8.0.38	123 /udp	service	ntp (123/UDP)			
10.8.0.38	1900 /udp	service	ssdp (1900/UDP)			
10.8.0.38	139 /tcp	info	OS=[Windows 7 Professional 7601 Service Pack 1] Server=[Windows 7 Professional 6.1]			
win-iqf3u12cja5.sainttest.local		concern	DNS server allows zone transfers	DNS	CVE-1999-0532	0.0
win-iqf3u12cja5.sainttest.local	1048 /tcp	concern	NFS export list disclosure	RPC		2.6
win-iqf3u12cja5.sainttest.local	389 /tcp	potential	Possible buffer overflow in Active Directory	Windows OS		2.6
win-iqf3u12cja5.sainttest.local	139 /tcp	potential	AV Information: Anti-virus software is not installed or its presence could not be checked	Other		2.6
win-iqf3u12cja5.sainttest.local	53/tcp	potential	DNS server allows recursive queries	DNS		2.6
win-iqf3u12cja5.sainttest.local		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
win-iqf3u12cja5.sainttest.local	389 /tcp	potential	Is your LDAP secure?	Other		2.6
win-iqf3u12cja5.sainttest.local	139 /tcp	potential	Windows null session domain SID disclosure	Windows OS	CVE-2000-1200	5.0
win-iqf3u12cja5.sainttest.local	139 /tcp	potential	Windows null session host SID disclosure	Windows OS		2.6
win-iqf3u12cja5.sainttest.local	3389	potential	Microsoft Terminal Server allows weak encryption	Other		2.6
win-iqf3u12cja5.sainttest.local	1039 /tcp	potential	rpc.statd is enabled and may be vulnerable	RPC	CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800	10.0
win-iqf3u12cja5.sainttest.local	111 /tcp	potential	The sunrpc portmapper service is running	Other	CVE-1999-0632	0.0
win-iqf3u12cja5.sainttest.local	111 /tcp	potential	sunrpc services may be vulnerable	RPC	CVE-2002-0391 CVE-2003-0028	10.0
win-iqf3u12cja5.sainttest.local	443 /tcp	potential	TCP timestamp requests enabled	Other		2.6
win-iqf3u12cja5.sainttest.local	135 /tcp	potential	Windows DNS Server RPC Management Interface Buffer Overflow	DNS	CVE-2007-1748	10.0
win-iqf3u12cja5.sainttest.local	53/tcp	service	DNS			
win-iqf3u12cja5.sainttest.local		service	NFS			
win-iqf3u12cja5.sainttest.local	139 /tcp	service	SMB			
win-iqf3u12cja5.sainttest.local	80/tcp	service	WWW			
win-iqf3u12cja5.sainttest.local	443 /tcp	service	WWW (Secure)			
win-iqf3u12cja5.sainttest.local	8082 /tcp	service	WWW (non-standard port 8082)			

win-iqf3u12cja5.sainttest.local	53 /udp	service	domain (53/UDP)
win-iqf3u12cja5.sainttest.local	135 /tcp	service	epmap (135/TCP)
win-iqf3u12cja5.sainttest.local	500 /udp	service	isakmp (500/UDP)
win-iqf3u12cja5.sainttest.local	88/tcp	service	kerberos (88/TCP)
win-iqf3u12cja5.sainttest.local	88 /udp	service	kerberos (88/UDP)
win-iqf3u12cja5.sainttest.local	389 /tcp	service	ldap (389/TCP)
win-iqf3u12cja5.sainttest.local	389 /udp	service	ldap (389/UDP)
win-iqf3u12cja5.sainttest.local	445 /tcp	service	microsoft-ds (445/TCP)
win-iqf3u12cja5.sainttest.local	3389 /tcp	service	ms-wbt-server (3389/TCP)
win-iqf3u12cja5.sainttest.local	3268 /tcp	service	msft-gc (3268/TCP)
win-iqf3u12cja5.sainttest.local	3269 /tcp	service	msft-gc-ssl (3269/TCP)
win-iqf3u12cja5.sainttest.local	138 /udp	service	netbios-dgm (138/UDP)
win-iqf3u12cja5.sainttest.local	137 /udp	service	netbios-ns (137/UDP)
win-iqf3u12cja5.sainttest.local	123 /udp	service	ntp (123/UDP)
win-iqf3u12cja5.sainttest.local	636 /tcp	service	ssl-ldap (636/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	service	sunrpc (111/TCP)
win-iqf3u12cja5.sainttest.local	111 /udp	service	sunrpc (111/UDP)
win-iqf3u12cja5.sainttest.local	4343 /tcp	service	unicall (4343/TCP)
win-iqf3u12cja5.sainttest.local	139 /tcp	info	Netbios Attribute: Domain Controller
win-iqf3u12cja5.sainttest.local	139 /tcp	info	Netbios Attribute: Master Browser
win-iqf3u12cja5.sainttest.local	139 /tcp	info	Netbios Attribute: Primary Domain Controller
win-iqf3u12cja5.sainttest.local	139 /tcp	info	OS=[Windows Server 2008 R2 Enterprise 7600] Server=[Windows Server 2008 R2 Enterprise 6.1]
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-2 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-2 portmapper (111/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-3 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-3 portmapper (111/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-4 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100000-4 portmapper (111/UDP)

win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100003-2 nfs (2049/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100003-2 nfs (2049/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100003-3 nfs (2049/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100003-3 nfs (2049/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-1 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-1 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-2 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-2 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-3 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100005-3 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-1 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-1 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-2 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-2 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-3 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-3 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-4 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100021-4 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100024-1 status (1039/TCP)
win-iqf3u12cja5.sainttest.local	111 /tcp	info	RPC service: 100024-1 status (1039/UDP)

4 Details

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

4.1 10.8.0.1

IP Address: 10.8.0.1 **Host type:** Cisco IOS 11.1
Scan time: Dec 14 20:04:49 2015

server is susceptible to BEAST attack

Severity: Potential Problem **CVE:** CVE-2011-3389

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1, and therefore isn't recommended.

Where can I read more about this?

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.
Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.
Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

Technical Details

Service: https
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_64_CBC_SHA

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
```

/pre> 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=803b2aa3

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: cisco-IOS

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-Cisco-1.25

SSH supports weak ciphers

Severity: Potential Problem

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Configure the SSH server not to support SSH1, and not to use the original DES encryption algorithm, or any other ciphers with a key length of less than 128 bits.

For OpenSSH servers, SSH1 can be disabled by placing the following line into the **`sshd_config`** file:

```
Protocol 2
```

The ciphers to use with the SSH2 protocol in OpenSSH or SSH Communications Security SSH Server can be specified using the **`Ciphers`** setting in the **`sshd_config`** or **`sshd2_config`** file. For more information see the SSH documentation. Note: all SSH2 ciphers currently supported by OpenSSH are already considered strong.

Where can I read more about this?

For more information on configuring SSH, see onlamp.com.

Technical Details

Service: ssh
Supported SSH1 ciphers: des 3des

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-Cisco-1.25

SSL certificate is self signed

Severity: Potential Problem

Impact

When a server's SSL certificate is invalid, clients cannot properly verify that the server is authentic, resulting in a lack of trust.

Resolution

For expired certificates, contact the issuer of your SSL certificate to renew your certificate.

For certificates where the subject does not match the target, change the registered DNS name of the site to match the certificate, or contact the issuer of your SSL certificate to get a corrected certificate.

Replace self-signed certificates with certificates issued by a trusted certificate authority.

For wildcard certificates, replace the wildcard certificates with certificates whose Common Names match the host they are intended to be used with.

Where can I read more about this?

For more information on certificates see the HOWTO.

Technical Details

Service: https
Issued To IOS-Self-Signed-Certificate-3563137889
Issued By IOS-Self-Signed-Certificate-3563137889

SSL server accepts weak ciphers

Severity: Potential Problem

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

For Apache mod_ssl web servers, use the **`SSLCipherSuite`** directive in the configuration file to specify strong ciphers only and disable SSLv2 and export ciphers.

For Microsoft IIS web servers, disable SSLv2 and any weak ciphers as described in Microsoft knowledge base articles 187498 and 245030.

For other types of web servers, consult the web server documentation.

Where can I read more about this?

For more information, see VNU Net: Weak Security Found in Many Web Servers.

Technical Details

Service: https
Supported ciphers: RC4-SHA:TLSv1/SSLv3:128-bit DES-CBC-SHA:TLSv1/SSLv3:56-bit

server is susceptible to SSL POODLE attack

Severity: Potential Problem **CVE:** CVE-2014-3566

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

SSLv3 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 entirely is another alternative, but may affect the usability of the web site. The **`TLS_FALLBACK_SCSV`** mechanism can also be used to mitigate the vulnerability if it is supported by both the client and the server.

To fix the vulnerability in the TLS implementation in F5 devices, see SOL15882.

Where can I read more about this?

The POODLE attack was described in The POODLE Bites: Exploiting the SSL 3.0 Fallback.

The POODLE attack against TLS implementations was reported by ImperialViolet.

Technical Details

Service: https
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_64_CBC_SHA

SSL/TLS server supports RC4 ciphers

Severity: Potential Problem **CVE:** CVE-2013-2566 CVE-2015-2808

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

For Apache mod_ssl web servers, add **`!RC4`** to the **`SSLCipherSuite`** directive in the configuration file to disable RC4 ciphers.

For Microsoft IIS web servers, disable RC4 ciphers as described in Microsoft knowledge base article 245030.

For other types of web servers, consult the web server documentation to find out how to disable RC4 ciphers.

Where can I read more about this?

For more information on the Invariance Weakness and Bar Mitzvah attack, see Security Affairs and Imperva's paper, Attacking SSL when using RC4.

For more information on the ciphertext bias weakness, see the blog post Attack of the Week: RC4 is kind of broken in TLS.

Technical Details

Service: https
Server accepted SSL 3.0 RC4 cipher: SSL3_CK_RSA_RC4_128_MD5

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

SSH

Severity: Service

Technical Details

SSH-1.99-Cisco-1.25

Telnet

Severity: Service

Technical Details

WWW

Severity: Service

Technical Details

HTTP/1.1 401 Unauthorized
Date: Tue, 15 Dec 2015 00:54:27 GMT
Server: cisco-IOS
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15 or view_access"
401

WWW (Secure)

Severity: Service

Technical Details

\022\003\000\000J\002\000\000F\003\000Vod\201\239K\2343\130\154\242l\236\012\244\251:\023\246\
234\251OviE\148l\007\228\128\212\174 \031\226H\007\175\007
/\182G\025n\174oT2\142\027d\006\253\160\022J\234\000\015\146\203\183\163\030\003\000

l2f (1701/UDP)

Severity: Service

Technical Details

4.2 win2003unpatch.sainttest.local

IP Address: 10.8.0.11
Scan time: Dec 15 06:10:47 2015

Host type: Windows Server 2003
Netbios Name: WIN2003UNPATCH

vulnerable Microsoft.NET Framework version: 1.1.4322

Severity: Area of Concern

CVE: CVE-2007-0041 CVE-2007-0042 CVE-2007-0043

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could cause a denial of service, execute arbitrary code, or gain unauthorized access to configuration files.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 3.5)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 12-035 (.NET Framework 1.1, 2.0, 3.5, 3.51, 4.0)
- 12-074 (.NET Framework 2.0, 3.5, 3.5.1, 4.0)
- 13-004
- 13-007 (.NET Framework 3.5, 3.5.1, 4.0)
- 13-015 (.NET Framework 2.0, 3.5, 3.5.1, 4.0, 4.5)
- 13-052 (.NET Framework 1.0, 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5)
- 13-082 (.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5)
- 14-046 (.NET Framework 2.0, 3.5, 3.5.1)
- 14-053 (.NET Framework 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5, 4.5.1, 4.5.2)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, 11-078, 11-100, 12-016, 12-025, 12-034, 12-035, 12-038, 12-074, 13-004, 13-007, 13-015, 13-040, 13-052, 13-082, 14-009, 14-026, 14-046, 14-053, 14-057, 14-059, 14-072, 15-041, 15-048, 15-044, 15-092, 15-101, 15-118.

Technical Details

Service: http
Sent: GET /s1a2i3n4.ashx HTTP/1.0
Host: win2003unpatch.sainttest.local
Received: X-AspNet-Version: 1.1.4322

Group Policy Code Execution Vulnerability (MS15-011)

Severity: Area of Concern

CVE: CVE-2015-0008

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
Group Policy Code Execution Vulnerability (MS15-011)	Fixes a code execution vulnerability that can be triggered when a user connects to a rogue network with a domain configured. (CVE 2015-0008)	**Vista:** KB3000483 KB3000483 (x64) **Windows Server 2008:** KB3000483 KB3000483 (x64) **Windows 7:** KB3000483 KB3000483 (x64) **Windows Server 2008 R2:** KB3000483 **Windows 8** KB3000483 KB3000483 (x64) **Windows 8.1** KB3000483 KB3000483 (x64) **Windows Server 2012** KB3000483 **Windows Server 2012 R2** KB3000483	15-011

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2, Windows 8.1, Windows 10, and Windows Server 2012 and Windows Server 2012 R2.

Technical Details

Service: netbios
No patch available for MS15-011 on Windows Server 2003

AV Information: Anti-virus software is not installed or its presence could not be checked

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
no registry access

Possible Microsoft IIS ASP Remote Code Execution vulnerability

Severity: Potential Problem **CVE:** CVE-2008-0075

Impact

An attacker could send a specially constructed request which crashes the server or executes arbitrary code with the privileges of the web server.

Resolutions

Install the patches referenced in Microsoft Security Bulletins 03-018, 06-034 (for Windows 2000), 08-062, and 10-065.

For IIS 5.1, also install the patches referenced in 07-041. Note that the patch referenced in Microsoft Security Bulletin 02-050 must also be installed if client side certificates are to function.

IIS 4.0 users should also install the patch referenced in Microsoft Security Bulletin 04-021 or disable the *permanent redirection* option under the *Home Directory* tab in the web site properties.

Where can I read more about this?

More information on the ASP Remote Code Execution vulnerability in Windows 2003 and XP is available in Microsoft Security Bulletin 08-006, (US) CERT Technical Alert TA08-043C, Hewlett-Packard security bulletin HPSBST02314 / SSRT080016, Secunia advisory 28893, Security Focus Bugtraq ID 27676, and Security

Tracker Alert ID 1019385.

Technical Details

Service: http
IIS 6 detected and cannot check for patch (credentials required)

Possible Microsoft IIS ASP Upload Command Execution vulnerability

Severity: Potential Problem **CVE:** CVE-2006-0026

Impact

An attacker could send a specially constructed request which crashes the server or executes arbitrary code with the privileges of the web server.

Resolutions

Install the patches referenced in Microsoft Security Bulletins 03-018, 06-034 (for Windows 2000), 08-062, and 10-065.

For IIS 5.1, also install the patches referenced in 07-041. Note that the patch referenced in Microsoft Security Bulletin 02-050 must also be installed if client side certificates are to function.

IIS 4.0 users should also install the patch referenced in Microsoft Security Bulletin 04-021 or disable the *permanent redirection* option under the *Home Directory* tab in the web site properties.

Where can I read more about this?

More information on the ASP Upload Command Execution vulnerability is available in Microsoft Security Bulletin 06-034, (US) CERT Vulnerability Note VU#395588, Neohapsis 2006 July message #0316, OSVDB record 27152, Secunia Advisory 21006, Security Focus Bugtraq ID 18858 and exploit, and Security Tracker Alert ID 1016466.

Technical Details

Service: http
IIS 6 detected and cannot check for patch (credentials required)

web server allows MIME sniffing

Severity: Potential Problem

Impact

An attacker may be able to cause arbitrary script to run in a user's browser in the context of the vulnerable site.

Resolution

All HTTP responses should include an accurate **`Content-Type`** header, and an **`X-Content-Type-Options: nosniff`** header. The latter header instructs browsers always to use the specified content type instead of performing MIME sniffing, and is currently supported by Internet Explorer and Chrome.

The **`X-Content-Type-Options: nosniff`** header can be set in the web server's configuration as follows:

- **Apache**:
  Add the following directive to the configuration file:

```
Header set X-Content-Type-Options "nosniff"
```

- **IIS**:
  In IIS Manager, navigate to the desired level. Go to Features View -> HTTP Response Headers -> Actions pane. Click Add. In the Add Custom HTTP Response Header dialog box, enter **`X-Content-Type-Options`** in the *Name* box, and **`nosniff`** in the *Value* box.

Where can I read more about this?

For more information about MIME-sniffing risks and defenses, see Wikipedia and IE8 Security Part V. (Scroll down to the *MIME-Handling Changes* section.)

Technical Details

Service: http
Sent:
GET / HTTP/1.0
Host: win2003unpatch.sainttest.local
User-Agent: Mozilla/5.0
Received:
Missing Content-Type header or X-Content-Type-Options header not set to nosniff

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
```

/pre> 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=91395e02

imap receives cleartext password

Severity: Potential Problem

Impact

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

Resolution

Disable the IMAP server and use a more secure protocol such as IMAPS. If IMAP 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: imap
Received:
* OK IMAPrev1
GET BAD Unknown or NULL command
BAD NULL COMMAND
QUIT BAD NULL COMMAND
BAD NULL COMMAND

Obsolete Windows Release: Windows Server 2003

Severity: Potential Problem

Impact

Security updates for the target's Windows release are no longer available, possibly leaving the target vulnerable to attacks.

Resolution

Systems should be upgraded to a supported version of Microsoft Windows (Windows Vista or higher).

Where can I read more about this?

The information found at Microsoft Support LifeCycle has been laid out in the "Timeline Of Windows" table at Microsoft Windows (Wikipedia).

Technical Details

Service: registry
Received: Server: Microsoft-IIS/6.0

pop receives password in clear

Severity: Potential Problem

Impact

Unauthorized users and/or malicious users exploiting this vulnerability may be able to gain access to the target system.

Resolution

The specification for **POP3** servers (RFC 1725) describes an optional command to help resolve this clear text password issue. When the initial connection is made to a **POP** server, the server displays a timestamp in its banner. The client uses this timestamp to create an MD5 hash string that is shared between the server and client. The next time the client connects to the server (e.g., to check for new mail) it will issue a command (**APOP**) and the hash string. This method reduces the number of times that a user's userid and password are transmitted in clear text.

An optional method (**IMAP4**), described in RFC 1734, provides another means of authentication. The AUTH command allows the client to specify an authentication mechanism to be used and a protocol exchange. This allows the client to specify authentication methods it knows about and challenge the server to see if it knows any of them as well. If no authentication method can be agreed upon, then the **APOP** command is used (RFC 1725).

Also, you may install the latest Secure **POP3** mail server (with **APOP**/**IMAP4**) or disable **POP** mail if necessary.

Where can I read more about this?

Read CERT Advisory 97.09 for more information on vulnerabilities found in IMAP and POP. Also, visit Eudora's Internet Messaging Primer for an overview on POP and IMAP.

Technical Details

Service: pop
Received: +OK POP3

SMTP receives cleartext password

Severity: Potential Problem

Impact

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

Resolution

Disable the LOGIN and PLAIN authentication mechanisms as follows:

- **Postfix:** Set **`smtpd_sasl_security_options`** to **`noplaintext`** in the **`main.cf`** file.
- **Exchange:** In Exchange System Manager, expand Servers -> your inbound Exchange server -> Protocols -> SMTP. Right-click your inbound SMTP virtual server, and then click Properties. Go to the Access tab, and then Authentication, and clear the Basic Authentication check box.
- **Other mail servers:** Consult your mail server's documentation.

Where can I read more about this?

See RFC 2554 and the SMTP Authentication Tutorial for more information on SMTP authentication.

See the Microsoft article for more information about disabling Basic authentication in Microsoft Exchange.

Technical Details

Service: 587:TCP
Received:
250 AUTH LOGIN

SMTP receives cleartext password

Severity: Potential Problem

Impact

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

Resolution

Disable the LOGIN and PLAIN authentication mechanisms as follows:

- **Postfix:** Set **`smtpd_sasl_security_options`** to **`noplaintext`** in the **`main.cf`** file.
- **Exchange:** In Exchange System Manager, expand Servers -> your inbound Exchange server -> Protocols -> SMTP. Right-click your inbound SMTP virtual server, and then click Properties. Go to the Access tab, and then Authentication, and clear the Basic Authentication check box.
- **Other mail servers:** Consult your mail server's documentation.

Where can I read more about this?

See RFC 2554 and the SMTP Authentication Tutorial for more information on SMTP authentication.

See the Microsoft article for more information about disabling Basic authentication in Microsoft Exchange.

Technical Details

Service: smtp

Received:
250 AUTH LOGIN

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:
<title ID=titletext>Under Construction</title>

587/TCP

Severity: Service

Technical Details

220 WIN2003UNPATCH ESMTP

1026/UDP

Severity: Service

Technical Details

1027/UDP

Severity: Service

Technical Details

IMAP

Severity: Service

Technical Details

* OK IMAPrev1

POP

Severity: Service

Technical Details

+OK POP3

SMB

Severity: Service

Technical Details

\131\000\000\001\143

SMTP

Severity: Service

Technical Details

220 WIN2003UNPATCH ESMTP

WWW

Severity: Service

Technical Details

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.8.0.11/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 23:48:30 GMT
Accept-Ranges:

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

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

4.3 xprounpatched.sainttest.local

IP Address: 10.8.0.14
Scan time: Dec 14 20:04:49 2015

Host type: Windows 2000
Netbios Name: XPPROUNPATCHED

Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

Severity: Critical Problem **CVE:** CVE-2012-0002 CVE-2012-0152

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
MS Remote Desktop Could Allow Remote Code Execution Vulnerabilities	Fixed Remote Code Execution Vulnerabilities in the Remote Desktop Protocol. If exploited, an attacker could run arbitrary code on the target system, then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2012-0002, CVE 2012-0152)	KB2621440 and KB2621402 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit, Itanium **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit, Itanium **2008 R2:** 64-bit(1), 64-bit(2), Itanium(1), Itanium(2) **Win 7:** 32-bit(1), 32-bit(2), 64-bit(1), 64-bit(2)	12-020

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2, Windows 8.1, Windows 10, and Windows Server 2012 and Windows Server 2012 R2.

Technical Details

Service: 3389
rdp server allows connect to unfreed channels. No error code at byte eight.

AV Information: Anti-virus software is not installed or its presence could not be checked

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
no registry access

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=13923300

Possible vulnerability in Microsoft Terminal Server

Severity: Potential Problem

CVE: CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218

Impact

Vulnerabilities in Microsoft Windows Terminal Server and Remote Desktop could allow a remote attacker to execute arbitrary code or crash the server, or could allow an attacker who is able to capture network traffic to decrypt sessions.

Resolution

There is no fix available to protect against the man-in-the-middle attack. Therefore, Terminal Services should only be used on trusted networks.

For Windows NT 4.0 Terminal Server Edition, apply the patches referenced in Microsoft Security Bulletins 00-087 and 01-052. There is no fix available for the denial of service vulnerability on Windows NT.

For Windows 2000, apply the patches referenced in Microsoft Security Bulletins 01-052, 02-051, and 05-041.

For Windows XP, apply the patches referenced in Microsoft Security Bulletins 02-051 and 05-041.

For Windows Server 2003, apply the patch referenced in Microsoft Security Bulletin 05-041.

For Citrix MetaFrame, download a hotfix from the Citrix Solution Knowledge Base, under *Hotfixes*.

It is also a good idea to filter TCP port 3389 at the firewall or router, such that only connections from legitimate users will be accepted.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 00-087, 01-052, 02-051, and 05-041, and Bugtraq.

For more information on the Citrix MetaFrame vulnerability, see the Bugtraq ID 3440.

Technical Details

Service: ms-wbt-server
port 3389/tcp open and KB899591 not applied or could not be checked

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

1026/UDP

Severity: Service

Technical Details

SMB

Severity: Service

Technical Details

\131\000\000\001\143

WWW

Severity: Service

Technical Details

HTTP/1.1 400 Bad Request
Content-Type: text/html
Server: Microsoft-HTTPAPI/1.0
Date: Tue, 15 Dec 2015 00:53:22 GMT
Connection: close
Content-Length: 39
<h1>Bad Request

blackjack (1025/UDP)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/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

ssdp (1900/UDP)

Severity: Service

Technical Details

4.4 saintvm64.sainttest.local

IP Address: 10.8.0.35
Scan time: Dec 14 20:04:49 2015

Host type: Ubuntu 12.04
Netbios Name: SAINTVM64

vulnerability in Samba 3.6.3

Severity: Critical Problem

CVE: CVE-2012-1182 CVE-2012-2111 CVE-2013-0454 CVE-2013-4124 CVE-2013-4408 CVE-2013-4475 CVE-2013-4496 CVE-2014-0178 CVE-2014-0244 CVE-2014-3493 CVE-2014-8143 CVE-2015-0240

Impact

A remote attacker could create accounts, read part of the credentials file, execute arbitrary commands, cause a denial of service, write to arbitrary files, gain elevated privileges, or disable logging of failed login attempts in a brute-force password attack.

Resolution

Upgrade to Samba 3.6.35 for 3.6.x, 4.0.25 for 4.0.x, 4.1.17 for 4.1.x, or higher when available.

Alternatively, apply a fix from your operating system vendor.

Where can I read more about this?

A list of all reported vulnerabilities affecting Samba is available from Samba.

The unexpected code execution in smbd was reported in Samba Security CVE-2015-0240.

The Active Directory Domain Controller Privilege Elevation was reported in Samba Security CVE-2014-8143.

The Samba two denial of service vulnerabilities were reported in Samba Security CVE-2014-0244 and Samba Security CVE-2014-3493.

The Samba uninitialized memory information disclosure vulnerability was reported in Samba Security CVE-2014-0178.

The Samba DCE-RPC packets handling buffer overflow vulnerability was reported in Secunia Advisory SA55966 and Samba Security CVE-2013-4496.

The Samba insecure file permissions and security bypass vulnerabilities were reported in Secunia Advisory SA55638.

The Packet Handling Denial of Service vulnerability was reported in Secunia Advisory SA54347.

The Samba CIFS attribute handling vulnerability was reported in Secunia Advisory SA52854.

The LSA RPC "take ownership" Privilege Security Bypass vulnerability was reported in Secunia Advisory SA48976.

The unauthenticated remote code execution vulnerability was reported in a Samba announcement.

The 3.x Multiple Unspecified Remote vulnerabilities were reported in Bugtraq ID 36250.

Technical Details

Service: netbios-ssn
Received: Samba 3.6.3

OpenSSH 5.9p1 is vulnerable

Severity: Area of Concern

CVE: CVE-2010-5107 CVE-2014-1692 CVE-2014-2532 CVE-2014-2653 CVE-2015-5352 CVE-2015-5600

Impact

Updated 09/04/15

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 7.1 or higher when available, or install a fix from your operating system vendor.

Where can I read more about this?

The OpenSSH keyboard-interactive authentication vulnerability was reported in OpenSSH Vulnerability Exposes Servers to Brute Force Attacks.

The XSECURITY restrictions bypass vulnerability was reported in OpenSSH Release 6.9.

The OpenSSH Client Rejected `HostCertificate` Handling Vulnerability and The OpenSSH `"child_set_env()"` Security Bypass Vulnerability were reported in DSA-2894-1.

The OpenSSH Connection Saturation Remote DoS vulnerability was reported in the oss-security list and as Bugtraq ID 58162.

Technical Details

Service: ssh

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=003bb1a1

NetBIOS share enumeration using null session

Severity: Potential Problem

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Shares: print$

Windows null session domain SID disclosure

Severity: Potential Problem **CVE:** CVE-2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**

Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Domain SID = S-1-5-21-2796322588-1385680984-3600811486

Windows null session host SID disclosure

Severity: Potential Problem

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Host SID = S-1-1459638016-4915282-5374023-5570639-80

excessive null session access

Severity: Potential Problem **CVE:** CVE-2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Got user list: nobody

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-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4

rpc.statd is enabled and may be vulnerable

Severity: Potential Problem

CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800

Impact

Several vulnerabilities in **statd** permit attackers to gain root privileges. They can be exploited by local users. They can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Resolution

One resolution to this vulnerability is to install vendor patches as they become available. For the format string bug, SUSE users should obtain the **nfs-utils** and package, version 0.1.9.1 or higher, from their vendor. For the String parsing error bug, Linux users should obtain the **nfs-utils** or **knfsdi** or **linuxnfs** packages, more detail information, please refer to SUSE Security Announcement web site. For the **SM_MON** buffer overflow, UnixWare users should obtain the patch.

Also, if **NFS** is not being used, there is no need to run **statd** and it can be disabled. The **statd** (or **rpc.statd**) program is often started in the system initialization scripts (such as /etc/rc* or /etc/rc*.d/*). If you do not require **statd** it should be commented out from the initialization scripts. In addition, any currently running **statd** processes should be identified using **ps(1)** and then terminated using **kill(1)**.

Where can I read more about this?

More information about the **statd/automountd** vulnerability is available in CERT Advisory 1999-05. You may read more about the **statd** buffer overflow in CERT Advisory 1997-26. The String parsing error vulnerability detail information can be found in CVE Details. The format string vulnerability was discussed in vendor bulletins from Red Hat, Debian, Mandrake, Trustix, and Conectiva, as well as CERT Advisory 2000.17. The **SM_MON** buffer overflow was announced in Caldera Security Advisory 2001-SCO.6. The file creation and removal vulnerability was discussed in CERT Advisory 1996-09.

Technical Details

Service: 47152:TCP

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

The sunrpc portmapper service is running

Severity: Potential Problem **CVE:** CVE-1999-0632

Impact

The sunrpc portmapper service is an unsecured protocol that tells clients which port corresponds to each RPC service. Access to port 111 allows the calling client to query and identify the ports where the needed server is running.

Resolution

Disable all unnecessary RPC services, which are typically enabled in /etc/inetd.conf and in the system boot

scripts, /etc/rc*, and to block high numbered ports at the network perimeter except for those which are needed.

Where can I read more about this?

More information can be obtained in, NVD for CVE-1999-0632.

Technical Details

Service: sunrpc
port 111/tcp is open

sunrpc services may be vulnerable

Severity: Potential Problem **CVE:** CVE-2002-0391 CVE-2003-0028

Impact

If an affected service is running, a remote attacker could execute arbitrary commands with *root* privileges.

Resolution

See CERT Advisories 2002-25 and 2003-10 for patch or upgrade information from your vendor. Note that it will be necessary to recompile statically linked applications after installing the patch or upgrade.

It would also be advisable to disable all unnecessary RPC services, which are typically enabled in **`/etc/inetd.conf`** and in the system boot scripts, **`/etc/rc*`**, and to block high numbered ports at the network perimeter except for those which are needed. Of particular importance are **`rpc.cmsd`**, **`dmispd`**, and **`kadmind`**, which are known to be exploitable and should be disabled or blocked.

Where can I read more about this?

These vulnerabilities were reported in CERT Advisories 2002-25 and 2003-10.

Technical Details

Service: sunrpc

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: sunrpc
timestamp=3035058119; uptime guess=140d 12h 17m 12s

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 (5)

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
5 < 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

SMB

Severity: Service

Technical Details

SSH

Severity: Service

Technical Details

SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4

microsoft-ds (445/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

sunrpc (111/TCP)

Severity: Service

Technical Details

sunrpc (111/UDP)

Severity: Service

Technical Details

4.5 10.8.0.38

IP Address: 10.8.0.38
Scan time: Dec 14 20:04:50 2015

Host type: Windows 7 SP1
Netbios Name: WIN7

vulnerable FileZilla server version: 0.9.41-beta

Severity: Area of Concern **CVE:** CVE-2014-0160 CVE-2014-0224

Impact

Vulnerabilities in FileZilla FTP server allow for a denial of service or attackers to obtain sensitive information.

Resolution

Upgrade to version 0.9.45 or higher.

Where can I read more about this?

The OpenSSL SSL/TLS handshake vulnerability was reported in FileZilla Server Version 0.9.45.

The OpenSSL vulnerability was reported in FileZilla Server Version 0.9.44.

Technical Details

Service: ftp
Received: 220-FileZilla Server version 0.9.41 beta

AV Information: Anti-virus software is not installed or its presence could not be checked

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
no registry access

server is susceptible to BEAST attack

Severity: Potential Problem **CVE:** CVE-2011-3389

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1, and therefore isn't recommended.

Where can I read more about this?

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.

Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.
Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

Technical Details

Service: ftp
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_192_CBC3_SHA

server is susceptible to BEAST attack

Severity: Potential Problem **CVE:** CVE-2011-3389

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1, and therefore isn't recommended.

Where can I read more about this?

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.
Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.
Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

Technical Details

Service: ms-wbt-server
Server accepted TLS 1.0 CBC cipher: TLS_RSA_WITH_AES_128_CBC_SHA

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-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
500 Syntax error, command unrecognized.
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:

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=50673900

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

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

server is susceptible to SSL POODLE attack

Severity: Potential Problem **CVE:** CVE-2014-3566

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

SSLv3 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 entirely is another alternative, but may affect the usability of the web site. The **TLS_FALLBACK_SCSV** mechanism can also be used to mitigate the vulnerability if it is supported by both the client and the server.

To fix the vulnerability in the TLS implementation in F5 devices, see SOL15882.

Where can I read more about this?

The POODLE attack was described in The POODLE Bites: Exploiting the SSL 3.0 Fallback.

The POODLE attack against TLS implementations was reported by ImperialViolet.

Technical Details

Service: ftp
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_192_CBC3_SHA

SSL/TLS server supports RC4 ciphers

Severity: Potential Problem **CVE:** CVE-2013-2566 CVE-2015-2808

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

For Apache mod_ssl web servers, add **!RC4** to the **SSLCipherSuite** directive in the configuration file to disable RC4 ciphers.

For Microsoft IIS web servers, disable RC4 ciphers as described in Microsoft knowledge base article 245030.

For other types of web servers, consult the web server documentation to find out how to disable RC4 ciphers.

Where can I read more about this?

For more information on the Invariance Weakness and Bar Mitzvah attack, see Security Affairs and Imperva's paper, Attacking SSL when using RC4.

For more information on the ciphertext bias weakness, see the blog post Attack of the Week: RC4 is kind of broken in TLS.

Technical Details

Service: ms-wbt-server
Server accepted TLS 1.0 RC4 cipher: TLS_RSA_WITH_RC4_128_SHA

SSL/TLS server supports RC4 ciphers

Severity: Potential Problem **CVE:** CVE-2013-2566 CVE-2015-2808

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

For Apache mod_ssl web servers, add **`!RC4`** to the **`SSLCipherSuite`** directive in the configuration file to disable RC4 ciphers.

For Microsoft IIS web servers, disable RC4 ciphers as described in Microsoft knowledge base article 245030.

For other types of web servers, consult the web server documentation to find out how to disable RC4 ciphers.

Where can I read more about this?

For more information on the Invariance Weakness and Bar Mitzvah attack, see Security Affairs and Imperva's paper, Attacking SSL when using RC4.

For more information on the ciphertext bias weakness, see the blog post Attack of the Week: RC4 is kind of broken in TLS.

Technical Details

Service: ftp
Server accepted SSL 3.0 RC4 cipher: SSL3_CK_RSA_RC4_128_MD5

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: netbios-ssn
timestamp=719772338; uptime guess=83d 7h 22m 3s

FTP

Severity: Service

Technical Details

220-FileZilla Server version 0.9.41 beta

SMB

Severity: Service

Technical Details

\131\000\000\001\143

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

\022\003\001\003H\002\000\000F\003\001Vod\144\200\191\029\212}\139}\007n\017_\007\154'W\134\
022\171R\177Es\132U\025\166'f
\028\006\000\000\237\240\144\166C\238S\026\012\1908\020u\216{\177\200\162'ELh\132\200_\153\2
46\001\000
/\000\011\000\002\246\000\002\243\000\002\2400\130\002\2360\130\001\212\160\003\002\001\002\0
02\016\024\146\203\189\225\209c\143G@\246w\0186\153\1960\006\t*\134H\134\247\001\001\005\005\
0000\0311\0290\027\006\003U\004\003\019\020Win7.SAINTtest.local0\030\023150817183448Z\023160216
183448Z0\0311\0290\027\006\003U\004\003\019\020Win7.SAINTtest.local0\130\001"0\006\t*\134H\134\
247\001\001\001\005\000\003\130\001\015\0000\130\001

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

ssdp (1900/UDP)

Severity: Service

Technical Details

4.6 win-iqf3u12cja5.sainttest.local

IP Address: 10.8.0.150
Scan time: Dec 14 20:04:49 2015

Host type: Windows Server 2008 R2
Netbios Name: WIN-IQF3U12CJA5

DNS server allows zone transfers

Severity: Area of Concern **CVE:** CVE-1999-0532

Impact

Attackers could collect information about the domain.

Resolution

Configure the primary DNS server to allow zone transfers only from secondary DNS servers. In BIND, this can be done in an **`allow-transfer`** block in the **`options`** section of the **`named.conf`** file.

Where can I read more about this?

Information on DNS zone transfers can be found here.

Information on securing DNS can be found here.

Technical Details

Service: dns
Received:
; <<>> DiG 9.8.1-P1 <<>> @win-iqf3u12cja5.sainttest.local SAINTTEST.local axfr
; (1 server found)
;; global options: +cmd
SAINTTEST.local.\x093600\x09IN\x09SOA\x09win-iqf3u12cja5.SAINTTEST.local.
hostmaster.SAINTTEST.local. 4889 900 600 86400 3600
SAINTTEST.local.\x09600\x09IN\x09A\x0910.8.0.150
SAINTTEST.local.\x093600\x09IN\x09NS\x09win-iqf3u12cja5.SAINTTEST.local.
_gc._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN\x09SRV 0 100 3268
win-iqf3u12cja5.sainttest.local.
_kerberos._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN SRV 0 100 88
win-iqf3u12cja5.sainttest.local.
_ldap._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN SRV 0 100 389
win-iqf3u12cja5.sainttest.local.
_gc._tcp.SAINTTEST.local. 600\x09IN\x09SRV\x090 100 3268 win-iqf3u12cja5.sainttest.local.
_kerberos._tcp.SAINTTEST.local.\x09600 IN\x09SRV\x090 100 88 win-iqf3u12cja5.sainttest.local.
_kpasswd._tcp.SAINTTEST.local. 600 IN\x09SRV\x090 100 464 win-iqf3u12cja5.sainttest.local.
_ldap._tcp.SAINTTEST.local. 600\x09IN\x09SRV\x090 100 389 win-iqf3u12cja5.sainttest.local.

NFS export list disclosure

Severity: Area of Concern

Impact

A remote attacker could view the list of exported file systems, which may contain sensitive information about the target's file system and trusted hosts.

Resolution

Disable the NFS service if it is not needed. If it is needed, block access to the mountd service at the firewall.

Where can I read more about this?

See Wikipedia for more information about NFS.

Technical Details

Service: 1048:TCP
Sent:
/sbin/showmount -e win-iqf3u12cja5.sainttest.local

Received:
Export list for win-iqf3u12cja5.sainttest.local:

Possible buffer overflow in Active Directory

Severity: Potential Problem

Impact

A remote attacker could crash the Active Directory service and force a reboot of the server. It may also be possible to execute commands on the server.

Resolution

Install the patches referenced in Microsoft Security Bulletin 15-096.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-039, 08-003, 08-035, 08-060, 09-018, 09-066, and 15-096.

Technical Details

Service: ldap

AV Information: Anti-virus software is not installed or its presence could not be checked

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
no registry access

DNS server allows recursive queries

Severity: Potential Problem

Impact

Allowing recursive queries may make the DNS server more susceptible to denial-of-service and cache poisoning attacks.

Resolution

Disable recursive queries on the DNS server.

For Windows DNS servers, this can be done by checking *Disable Recursion* from Start -> Control Panel -> Administrative Tools -> DNS -> Properties -> Advanced -> Server Options.

For BIND DNS servers, add the following line to the *options* section of the **`named.conf`** file:

```
recursion no;
```

Where can I read more about this?

For more information about the risks of recursive queries, see the Go Daddy Help Center.

Technical Details

Service: domain
Recursion Available flag = 1

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
```

/pre> 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=b8794100

Is your LDAP secure?

Severity: Potential Problem

Impact

If an application uses a vulnerable implementation of LDAP, an attacker could cause a denial of service or execute arbitrary commands.

Resolution

See CERT Advisory 2001-18 for information on obtaining a patch for your application. OpenLDAP 2.x users may also need to fix a separate set of vulnerabilities which were reported in SuSE Security Announcement 2002:047. Consult your vendor for a fix.

If a patch is not available, then ports 389 and 636, TCP and UDP, should be blocked at the network perimeter until a patch can be applied.

Where can I read more about this?

For more information, see CERT Advisory 2001-18 and SuSE Security Announcement 2002:047.

Technical Details

Service: ldap

Windows null session domain SID disclosure

Severity: Potential Problem **CVE:** CVE-2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **`regedt32`** command can be used for this

purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Domain SID = S-1-5-21-1092970315-2611599247-3581362680

Windows null session host SID disclosure

Severity: Potential Problem

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**

Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Host SID = S-1-5-21-1092970315-2611599247-3581362680

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

rpc.statd is enabled and may be vulnerable

Severity: Potential Problem

CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800

Impact

Several vulnerabilities in **statd** permit attackers to gain root privileges. They can be exploited by local users. They can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Resolution

One resolution to this vulnerability is to install vendor patches as they become available. For the format string bug, SUSE users should obtain the **nfs-utils** and package, version 0.1.9.1 or higher, from their vendor. For the String parsing error bug, Linux users should obtain the **nfs-utils** or **knfsdi** or **linuxnfs** packages, more detail information, please refer to SUSE Security Announcement web site. For the **SM_MON** buffer overflow, UnixWare users should obtain the patch.

Also, if **NFS** is not being used, there is no need to run **statd** and it can be disabled. The **statd** (or **rpc.statd**) program is often started in the system initialization scripts (such as /etc/rc* or /etc/rc*.d/*). If you do not require **statd** it should be commented out from the initialization scripts. In addition, any currently running **statd** processes should be identified using **ps(1)** and then terminated using **kill(1)**.

Where can I read more about this?

More information about the **statd/automountd** vulnerability is available in CERT Advisory 1999-05. You may read more about the **statd** buffer overflow in CERT Advisory 1997-26. The String parsing error vulnerability detail information can be found in CVE Details. The format string vulnerability was discussed in vendor bulletins from Red Hat, Debian, Mandrake, Trustix, and Conectiva, as well as CERT Advisory 2000.17. The **SM_MON** buffer overflow was announced in Caldera Security Advisory 2001-SCO.6. The file creation and removal vulnerability was discussed in CERT Advisory 1996-09.

Technical Details

Service: 1039:TCP

The sunrpc portmapper service is running

Severity: Potential Problem **CVE:** CVE-1999-0632

Impact

The sunrpc portmapper service is an unsecured protocol that tells clients which port corresponds to each RPC service. Access to port 111 allows the calling client to query and identify the ports where the needed server is running.

Resolution

Disable all unnecessary RPC services, which are typically enabled in /etc/inetd.conf and in the system boot scripts, /etc/rc*, and to block high numbered ports at the network perimeter except for those which are needed.

Where can I read more about this?

More information can be obtained in, NVD for CVE-1999-0632.

Technical Details

Service: sunrpc

port 111/tcp is open

sunrpc services may be vulnerable

Severity: Potential Problem **CVE:** CVE-2002-0391 CVE-2003-0028

Impact

If an affected service is running, a remote attacker could execute arbitrary commands with *root* privileges.

Resolution

See CERT Advisories 2002-25 and 2003-10 for patch or upgrade information from your vendor. Note that it will be necessary to recompile statically linked applications after installing the patch or upgrade.

It would also be advisable to disable all unnecessary RPC services, which are typically enabled in **`/etc/inetd.conf`** and in the system boot scripts, **`/etc/rc*`**, and to block high numbered ports at the network perimeter except for those which are needed. Of particular importance are **`rpc.cmsd`**, **`dmispd`**, and **`kadmind`**, which are known to be exploitable and should be disabled or blocked.

Where can I read more about this?

These vulnerabilities were reported in CERT Advisories 2002-25 and 2003-10.

Technical Details

Service: sunrpc

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: https
timestamp=45814956; uptime guess=5d 8h 32m 57s

Windows DNS Server RPC Management Interface Buffer Overflow

Severity: Potential Problem **CVE:** CVE-2007-1748

Impact

The Windows DNS Server has a vulnerability that allows for remote code execution.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 15-127.

Windows Server 2008 and Windows Server 2008 R2 users should apply the patch referenced in Microsoft Security Bulletin 09-008.

For the management interface buffer overflow, remote management over RPC can be disabled by setting the value of `RpcProtocol` in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters` to 4. Setting this value to 0 will disable all DNS RPC functionality and will protect against both local and remote attempts to exploit the vulnerability.

Where can I read more about this?

For more information on specific vulnerabilities, see Microsoft Security Bulletins 07-029, 07-062, 09-008, 11-058, 12-017, and 15-127. The DNS server RPC management interface buffer overflow was reported in US-CERT Vulnerability Note VU#555920 and Secunia Advisory SA24871.

Technical Details

Service: 135:TCP
Windows DNS Server port open

DNS

Severity: Service

Technical Details

NFS

Severity: Service

Technical Details

1048:TCP

SMB

Severity: Service

Technical Details

\131\000\000\001\143

WWW

Severity: Service

Technical Details

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 15 Dec 2015 00:53:24 GMT
Connection: close
Content-Length:

WWW (Secure)

Severity: Service

Technical Details

WWW (non-standard port 8082)

Severity: Service

Technical Details

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 15 Dec 2015 00:53:24 GMT
Connection: close
Content-Length:

domain (53/UDP)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

kerberos (88/TCP)

Severity: Service

Technical Details

kerberos (88/UDP)

Severity: Service

Technical Details

ldap (389/TCP)

Severity: Service

Technical Details

ldap (389/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

msft-gc (3268/TCP)

Severity: Service

Technical Details

msft-gc-ssl (3269/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

ssl-ldap (636/TCP)

Severity: Service

Technical Details

sunrpc (111/TCP)

Severity: Service

Technical Details

sunrpc (111/UDP)

Severity: Service

Technical Details

unicall (4343/TCP)

Severity: Service

Technical Details