SAINT IAVA Scan Report

Report Generated: December 14, 2015

1 Introduction

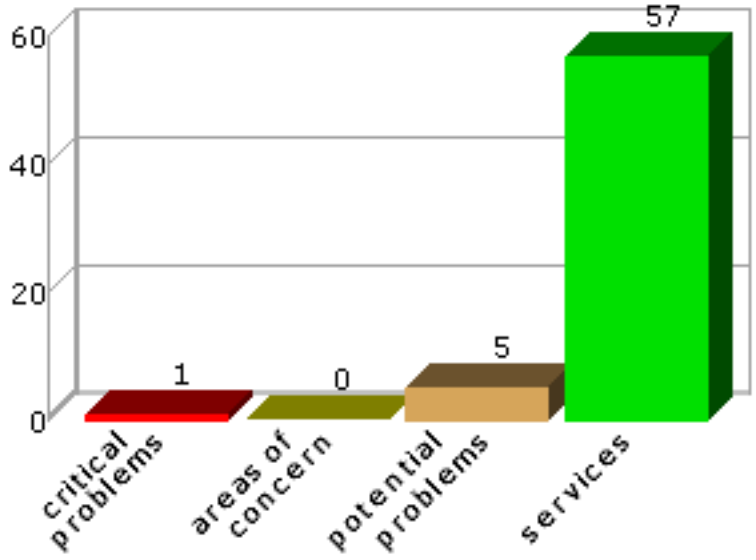
On December 14, 2015, at 12:51 PM, an IAVA assessment was conducted using the SAINT 8.9.28 vulnerability scanner. The scan discovered a total of three live hosts, and detected one critical problem, zero areas of concern, and five potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

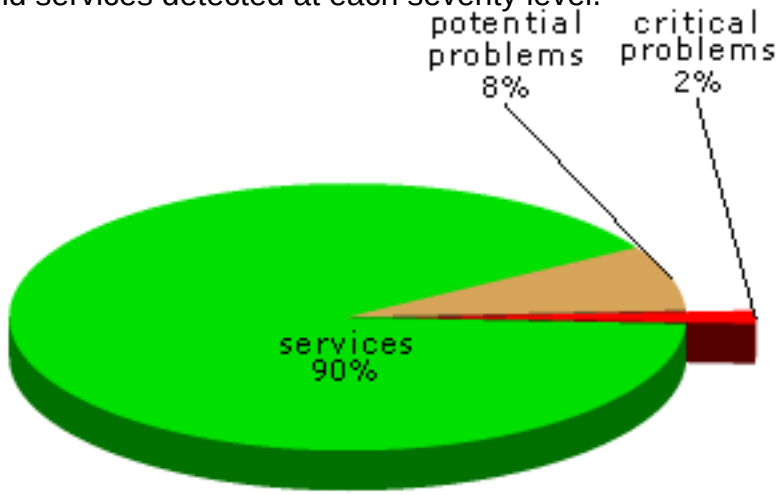
2 Summary

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

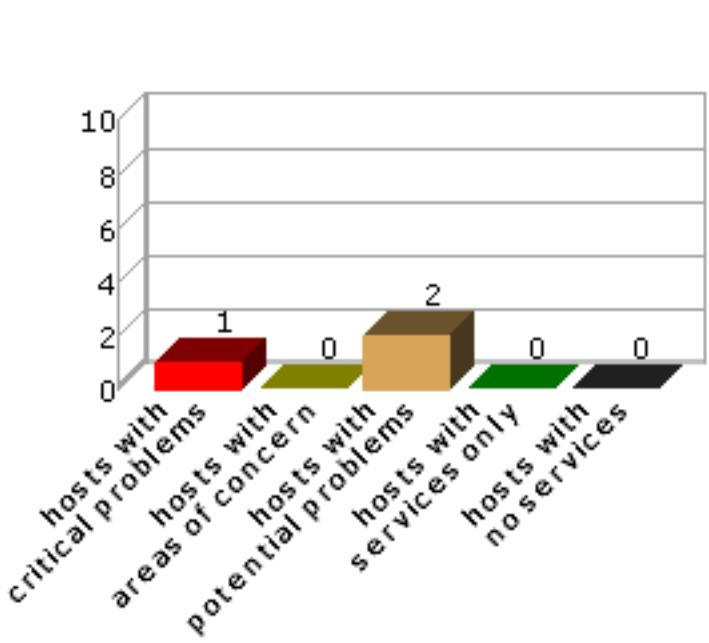
This section shows the overall number of vulnerabilities and services detected at each severity level.

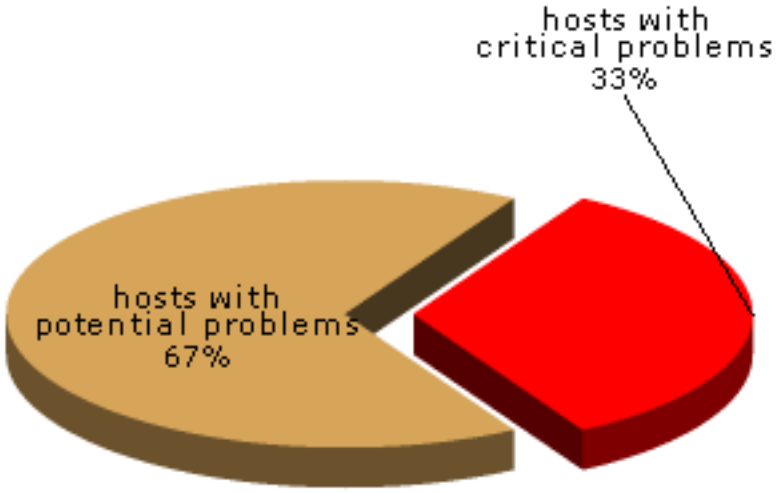




2.2 Hosts by Severity

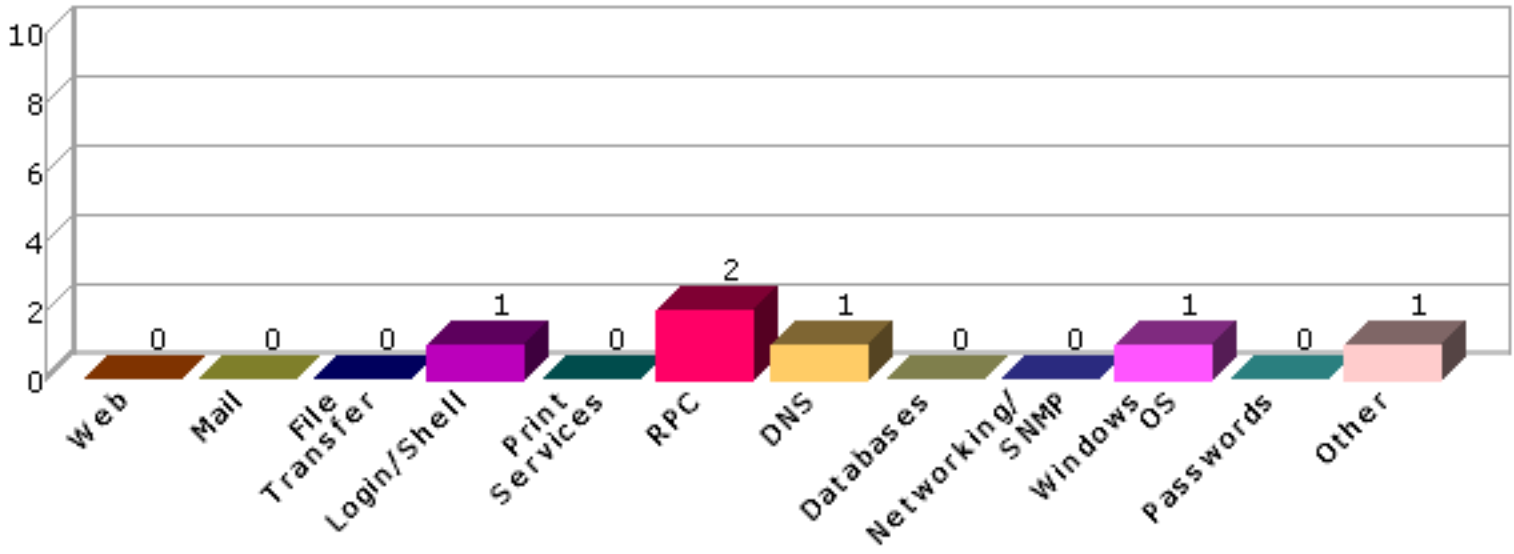
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

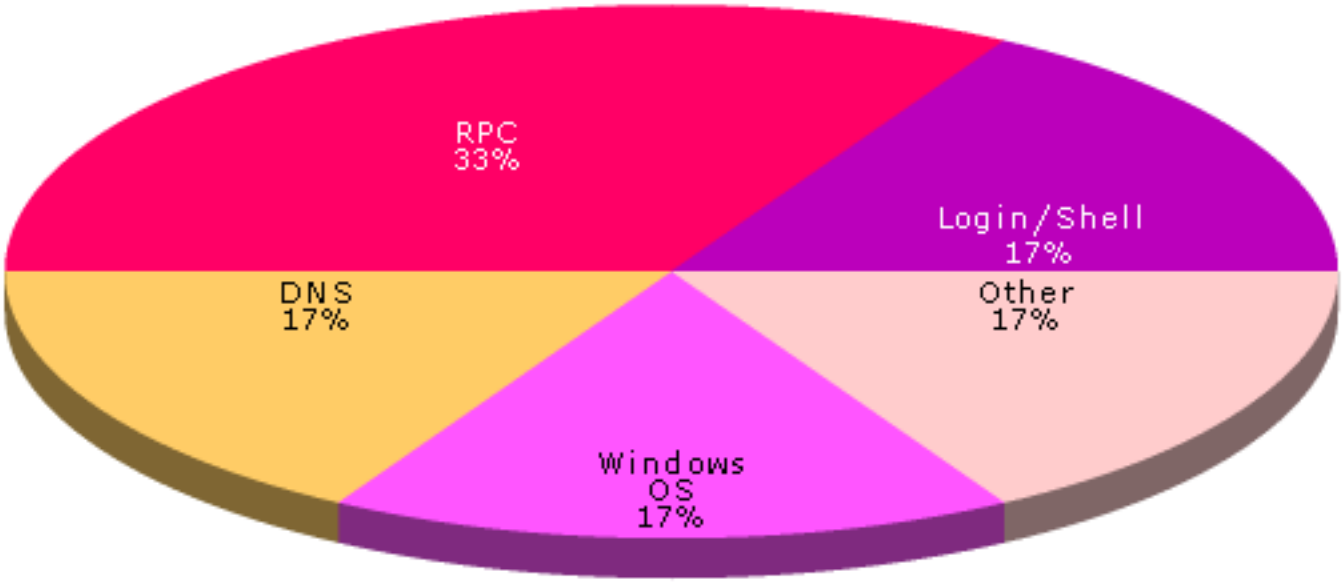




2.3 Vulnerabilities by Class

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





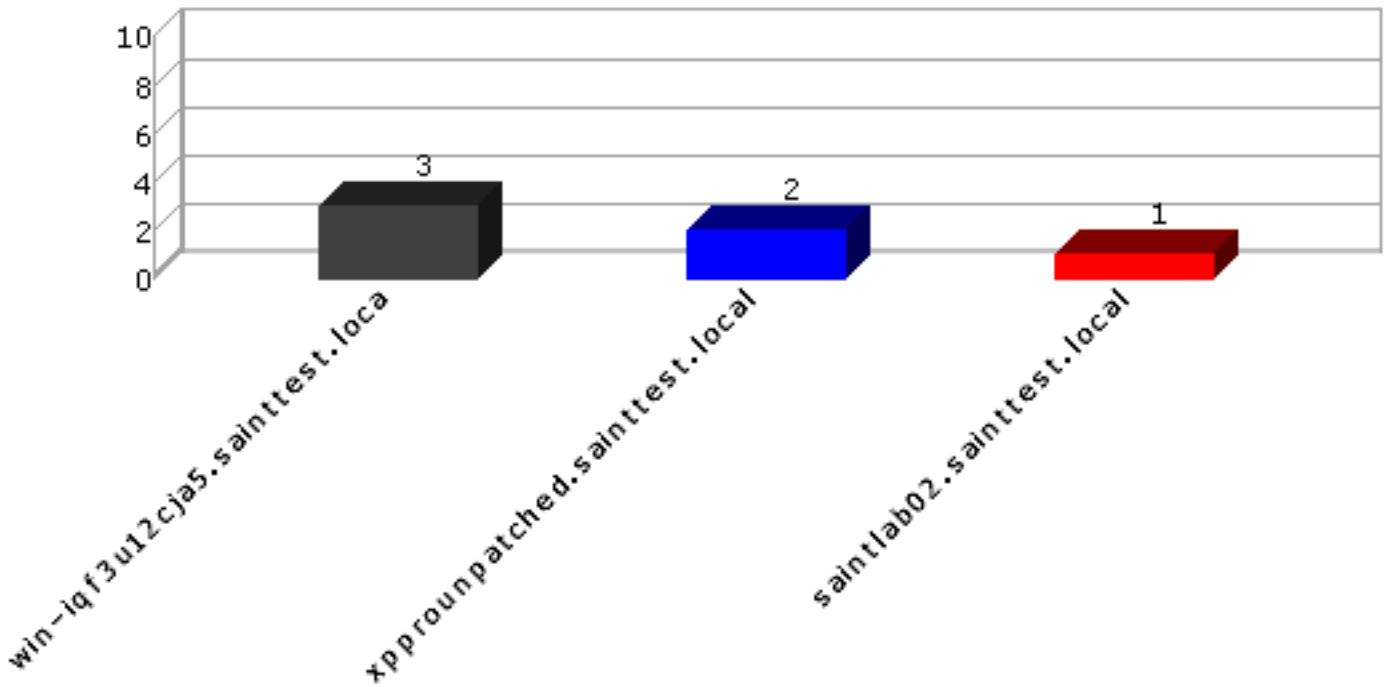
2.4 Hosts by Needed Patches

This section shows the number of hosts detected with various numbers of missing patches.

	# Hosts
Fully patched	1
1 patch needed	0
2 patches needed	2
3-4 patches needed	0
5+ patches needed	0
Total	3

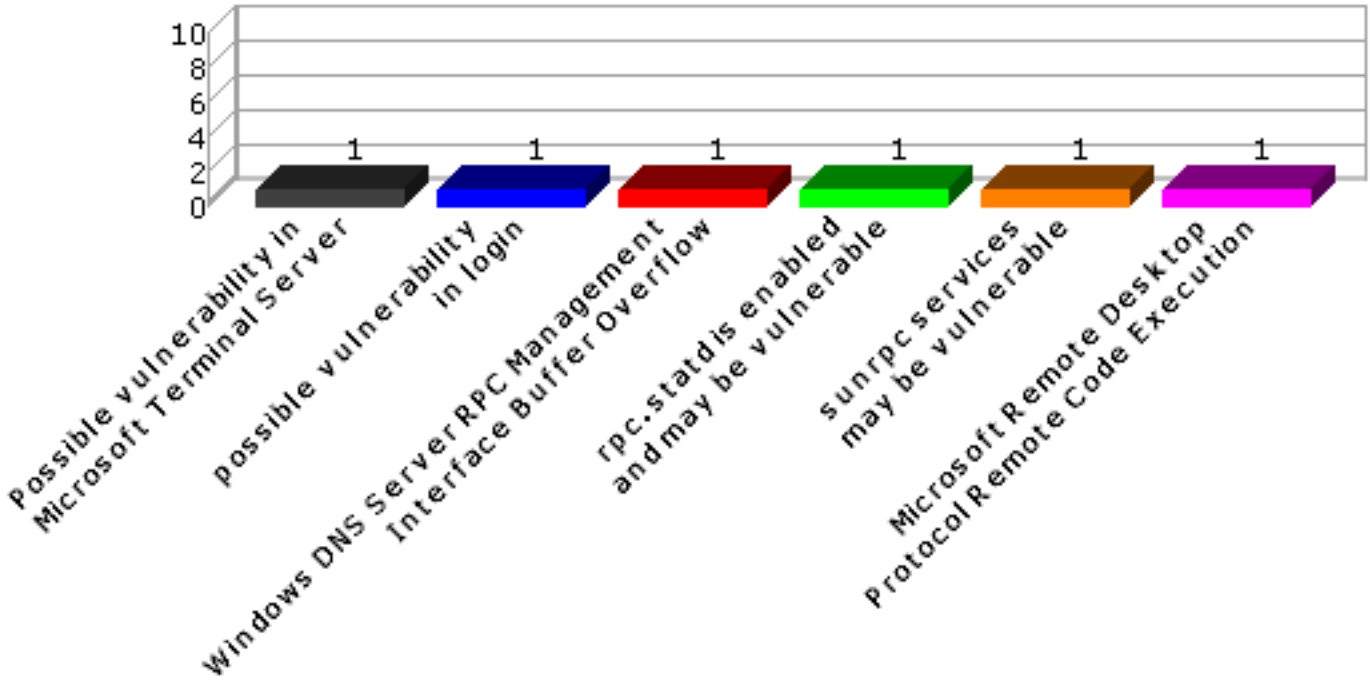
2.5 Top 10 Vulnerable Hosts

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



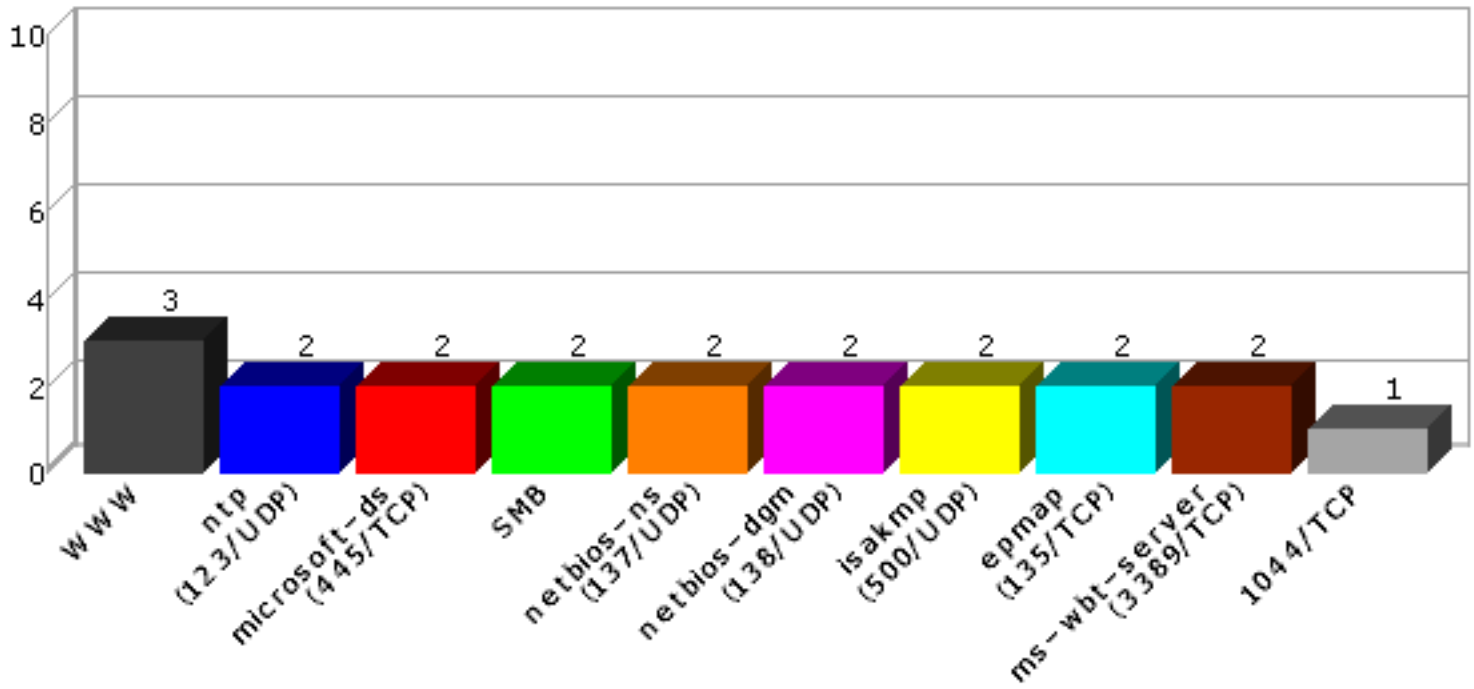
2.6 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, and the number of occurrences.



2.7 Top 10 Services

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



2.8 Top 10 Patches

This section shows the most commonly detected missing patches, and the number of hosts on which they are needed.

#	Patch	Hosts
1	MS12-020	1
2	MS02-057	1
3	MS05-041	1
4	MS07-029	1

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
saintlab02.sainttest.local		10.8.0.2		0	0	1
xpprounpatched.sainttest.local	XPPROUNPATCHED	10.8.0.14	Windows 2000 SP4	1	0	1
win-iqf3u12cja5.sainttest.local	WIN-IQF3U12CJA5	10.8.0.150	Windows Server 2008 R2	0	0	3

3.2 Vulnerability List

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

Host Name	Severity	Vulnerability / Service	Class	CVE	IAVA
saintlab02.sainttest.local	potential	possible vulnerability in login	Login /Shell	CVE-2001-0797	IAVA-2001-A-0014
saintlab02.sainttest.local	service	Telnet			
saintlab02.sainttest.local	service	WWW			
saintlab02.sainttest.local	service	bootps (67/UDP)			
xpprounpatched.sainttest.local	critical	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)	Windows OS	CVE-2012-0002 CVE-2012-0152	IAVA-2012-A-0039
xpprounpatched.sainttest.local	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	IAVA-2005-T-0026
xpprounpatched.sainttest.local	service	SMB			
xpprounpatched.sainttest.local	service	WWW			
xpprounpatched.sainttest.local	service	epmap (135/TCP)			
xpprounpatched.sainttest.local	service	isakmp (500/UDP)			
xpprounpatched.sainttest.local	service	microsoft-ds (445/TCP)			
xpprounpatched.sainttest.local	service	ms-wbt-server (3389/TCP)			
xpprounpatched.sainttest.local	service	netbios-dgm (138/UDP)			
xpprounpatched.sainttest.local	service	netbios-ns (137/UDP)			
xpprounpatched.sainttest.local	service	ntp (123/UDP)			
win-iqf3u12cja5.sainttest.local	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	IAVA-1999-A-0006 IAVA-2000-B-0005 IAVA-96-12 IAVA-97-12
win-iqf3u12cja5.sainttest.local	potential	sunrpc services may be vulnerable	RPC	CVE-2002-0391 CVE-2003-0028	IAVA-2002-T-0015 IAVA-2003-T-0007
win-iqf3u12cja5.sainttest.local	potential	Windows DNS Server RPC Management Interface Buffer Overflow	DNS	CVE-2007-1748	IAVA-2007-A-0027 IAVA-2007-A-0028
win-iqf3u12cja5.sainttest.local	service	1026/TCP			

win-iqf3u12cja5.sainttest.local	service	1027/TCP
win-iqf3u12cja5.sainttest.local	service	1029/TCP
win-iqf3u12cja5.sainttest.local	service	1033/TCP
win-iqf3u12cja5.sainttest.local	service	1039/TCP
win-iqf3u12cja5.sainttest.local	service	1044/TCP
win-iqf3u12cja5.sainttest.local	service	9389/TCP
win-iqf3u12cja5.sainttest.local	service	DNS
win-iqf3u12cja5.sainttest.local	service	NFS
win-iqf3u12cja5.sainttest.local	service	SMB
win-iqf3u12cja5.sainttest.local	service	WWW
win-iqf3u12cja5.sainttest.local	service	WWW (Secure)
win-iqf3u12cja5.sainttest.local	service	WWW (non-standard port 5985)
win-iqf3u12cja5.sainttest.local	service	WWW (non-standard port 8059)
win-iqf3u12cja5.sainttest.local	service	WWW (non-standard port 8082)
win-iqf3u12cja5.sainttest.local	service	blackjack (1025/TCP)
win-iqf3u12cja5.sainttest.local	service	cma (1050/TCP)
win-iqf3u12cja5.sainttest.local	service	domain (53/UDP)
win-iqf3u12cja5.sainttest.local	service	epmap (135/TCP)
win-iqf3u12cja5.sainttest.local	service	http-rpc-epmap (593/TCP)
win-iqf3u12cja5.sainttest.local	service	iad1 (1030/TCP)
win-iqf3u12cja5.sainttest.local	service	iad2 (1031/TCP)
win-iqf3u12cja5.sainttest.local	service	isakmp (500/UDP)
win-iqf3u12cja5.sainttest.local	service	iscsi-target (3260/TCP)
win-iqf3u12cja5.sainttest.local	service	kerberos (88/TCP)
win-iqf3u12cja5.sainttest.local	service	kerberos (88/UDP)
win-iqf3u12cja5.sainttest.local	service	kpasswd (464/TCP)
win-iqf3u12cja5.sainttest.local	service	ldap (389/TCP)
win-iqf3u12cja5.sainttest.local	service	m4-network-as (4345/TCP)
win-iqf3u12cja5.sainttest.local	service	microsoft-ds (445/TCP)
win-iqf3u12cja5.sainttest.local	service	ms-wbt-server (3389/TCP)
win-iqf3u12cja5.sainttest.local	service	msft-gc (3268/TCP)
win-iqf3u12cja5.sainttest.local	service	msft-gc-ssl (3269/TCP)
win-iqf3u12cja5.sainttest.local	service	neod1 (1047/TCP)
win-iqf3u12cja5.sainttest.local	service	neod2 (1048/TCP)
win-iqf3u12cja5.sainttest.local	service	netbios-dgm (138/UDP)
win-iqf3u12cja5.sainttest.local	service	netbios-ns (137/UDP)
win-iqf3u12cja5.sainttest.local	service	ntp (123/UDP)
win-iqf3u12cja5.sainttest.local	service	obrpd (1092/TCP)
win-iqf3u12cja5.sainttest.local	service	proofd (1093/TCP)
win-iqf3u12cja5.sainttest.local	service	shilp (2049/TCP)
win-iqf3u12cja5.sainttest.local	service	ssl-ldap (636/TCP)
win-iqf3u12cja5.sainttest.local	service	sunrpc (111/TCP)
win-iqf3u12cja5.sainttest.local	service	sunrpc (111/UDP)
win-iqf3u12cja5.sainttest.local	service	unicall (4343/TCP)
win-iqf3u12cja5.sainttest.local	info	Netbios Attribute: Domain Controller
win-iqf3u12cja5.sainttest.local	info	Netbios Attribute: Master Browser
win-iqf3u12cja5.sainttest.local	info	Netbios Attribute: Primary Domain Controller

win-iqf3u12cja5.sainttest.local	info	OS=[Windows Server 2008 R2 Enterprise 7600] Server=[Windows Server 2008 R2 Enterprise 6.1]
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-2 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-2 portmapper (111/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-3 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-3 portmapper (111/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-4 portmapper (111/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100000-4 portmapper (111/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100003-2 nfs (2049/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100003-2 nfs (2049/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100003-3 nfs (2049/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100003-3 nfs (2049/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-1 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-1 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-2 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-2 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-3 mountd (1048/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100005-3 mountd (1048/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-1 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-1 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-2 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-2 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-3 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-3 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-4 nlockmgr (1047/TCP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100021-4 nlockmgr (1047/UDP)
win-iqf3u12cja5.sainttest.local	info	RPC service: 100024-1 status (1039/TCP)
win-iqf3u12cja5.sainttest.local	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 saintlab02.sainttest.local

IP Address: 10.8.0.2
Scan time: Dec 14 12:51:46 2015

possible vulnerability in login

Severity: Potential Problem **CVE:** CVE-2001-0797

Impact

An unauthenticated remote user could gain root privileges on the system.

Resolution

See CERT Advisory 2001-34 for information on obtaining patches for your particular operating system.

If a patch is not yet available, then TCP ports 23 (**`telnet`**), 513 (**`rlogin`**), and any other services which rely on **`login`** should be blocked at the network perimeter or, better yet, shut off and replaced by a more secure alternative such as Secure Shell (**`ssh`**). When installing Secure Shell, ensure that the **`UseLogin`** option is shut off.

Where can I read more about this?

This vulnerability was reported in CERT Advisory 2001-34.

Technical Details

Service: login

Telnet

Severity: Service

Technical Details

WWW

Severity: Service

Technical Details

HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jul 1993 01:58:27 GMT
Server: cisco-IOS
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15_access"
401

bootps (67/UDP)

Severity: Service

Technical Details

4.2 xpprounpatched.sainttest.local

IP Address: 10.8.0.14
Scan time: Dec 14 12:51:46 2015

Host type: Windows 2000 SP4
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.

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

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: Mon, 14 Dec 2015 17:40:27 GMT
Connection: close
Content-Length: 39
<h1>Bad Request

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

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 win-iqf3u12cja5.sainttest.local

IP Address: 10.8.0.150
Scan time: Dec 14 12:51:46 2015
Host type: Windows Server 2008 R2
Netbios Name: WIN-IQF3U12CJA5

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

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

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

1026/TCP

Severity: Service

Technical Details

1027/TCP

Severity: Service

Technical Details

1029/TCP

Severity: Service

Technical Details

1033/TCP

Severity: Service

Technical Details

1039/TCP

Severity: Service

Technical Details

1044/TCP

Severity: Service

Technical Details

9389/TCP

Severity: Service

Technical Details

\008Ihttp://schemas.microsoft.com/ws/2006/05/framing/faults/UnsupportedVersion

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: Mon, 14 Dec 2015 17:40:27 GMT
Connection: close
Content-Length:

WWW (Secure)

Severity: Service

Technical Details

WWW (non-standard port 5985)

Severity: Service

Technical Details

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 14 Dec 2015 17:40:33 GMT
Connection: close
Content-Length:

WWW (non-standard port 8059)

Severity: Service

Technical Details

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 14 Dec 2015 17:40:36 GMT
Connection: close
Content-Length:

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: Mon, 14 Dec 2015 17:40:36 GMT
Connection: close
Content-Length:

blackjack (1025/TCP)

Severity: Service

Technical Details

cma (1050/TCP)

Severity: Service

Technical Details

domain (53/UDP)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

http-rpc-epmap (593/TCP)

Severity: Service

Technical Details

ncacn_http/1.0

iad1 (1030/TCP)

Severity: Service

Technical Details

ncacn_http/1.0

iad2 (1031/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

iscsi-target (3260/TCP)

Severity: Service

Technical Details

kerberos (88/TCP)

Severity: Service

Technical Details

kerberos (88/UDP)

Severity: Service

Technical Details

kpasswd (464/TCP)

Severity: Service

Technical Details

ldap (389/TCP)

Severity: Service

Technical Details

m4-network-as (4345/TCP)

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

neod1 (1047/TCP)

Severity: Service

Technical Details

neod2 (1048/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

obrpd (1092/TCP)

Severity: Service

Technical Details

proofd (1093/TCP)

Severity: Service

Technical Details

shilp (2049/TCP)

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

Scan Session: IAVA vuln scan; Scan Policy: IAVA; Scan Data Set: 14 December 2015 12:51