NERC CIP Vulnerability Assessment Report

Report Generated: December 14, 2015

1 Background

NERC introduced its Critical Infrastructure Protection (CIP) Reliability Standards CIP-002-1 through CIP-009-1 in 2006. In 2009, it approved version 2 of these standards and began auditing Registered Entities for compliance. All Registered Entities must comply with these eight categories of controls for securing critical cyber assets used to protect the bulk electric system. They include: Cyber Asset Identification, Security Management Controls, Personnel & Training, Electronic Security Perimeter(s), Physical Security, Systems Security Management, Incident Reporting and Response, and Recovery Plans for Critical Cyber Assets. Verification of compliance with CIP shows that a Registered Entity is providing optimal protection for the bulk electric system.

2 About this Report

On December 14, 2015, at 1:08 PM, a NERC CIP assessment was conducted on the following hosts. The results in the Summary section below document the findings from this scan, to include details about the host, vulnerabilities found, and Common Vulnerability Scoring System (CVSS) numerical score. This scan discovered a total of three live hosts and detected one critical problem, two areas of concern and 22 potential problems. The execution of this vulnerability scan and report directly fulfills CIP requirements for scanning for vulnerabilities in critical cyber assets for the following controls:

CIP-002 Critical Cyber Asset Identification
Identify and document a risk-based assessment method that will be used to identify critical assets. R2 requires an identifiable list and annual asset list review to update all critical cyber assets. Management will approve the list of critical cyber assets. A third-party, without vested interest, shall monitor the compliance to CIP002 outcome of NERC.

CIP-005 Cyber Electronic Security Perimeter(s)
Requires the identification and protection of the Electronic Security Perimeter(s) and Access Points where Cyber Assets reside (R1 and R4).

CIP-007 Cyber Systems Security Management
Define methods, processes and procedures for securing those systems determined to be Critical Cyber Assets (R1 and R3).Document technical and procedural controls to enforce authentication, accountability and user activity (R5). Finally, a third party annual review is required of the perimeter (R8).

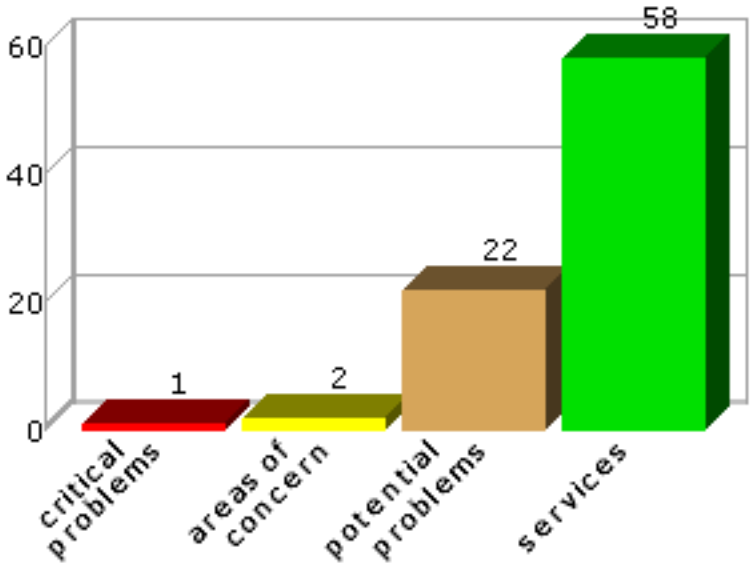
The Summary and Details sections provide comprehensive information related to the vulnerabilities - to include content to assess risk and determine remediation.

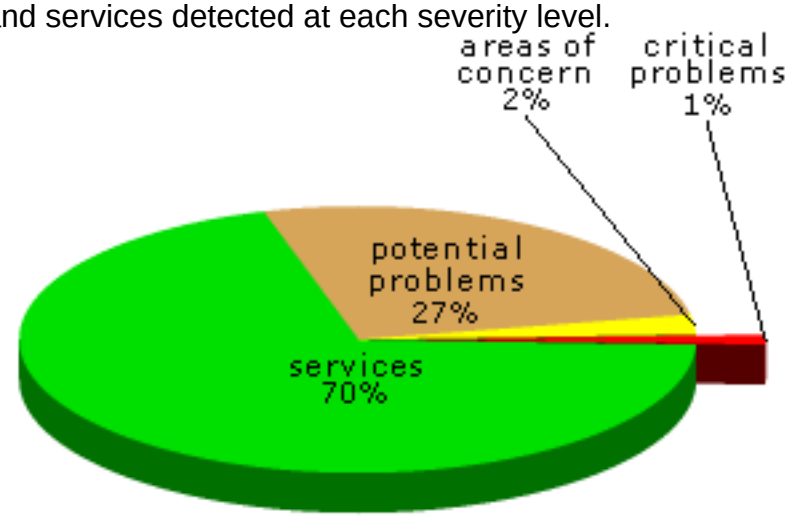
3 Summary

The sections below summarize the results of the scan.

3.1 Vulnerabilities by Severity

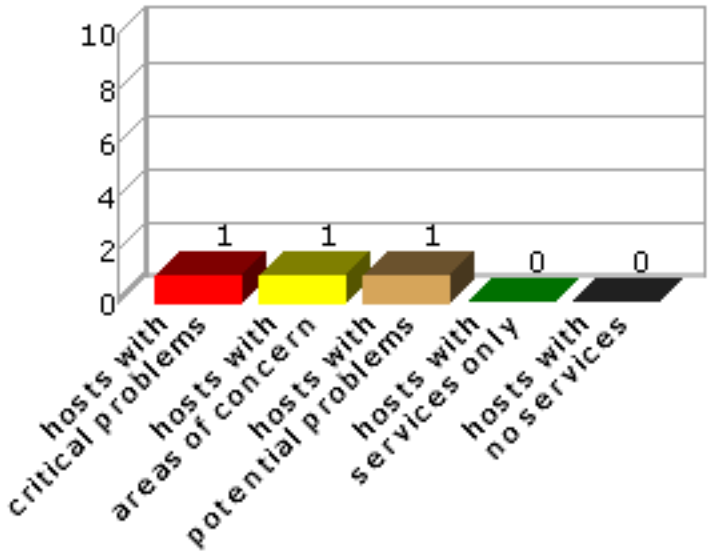
This section shows the overall number of vulnerabilities and services detected at each severity level.

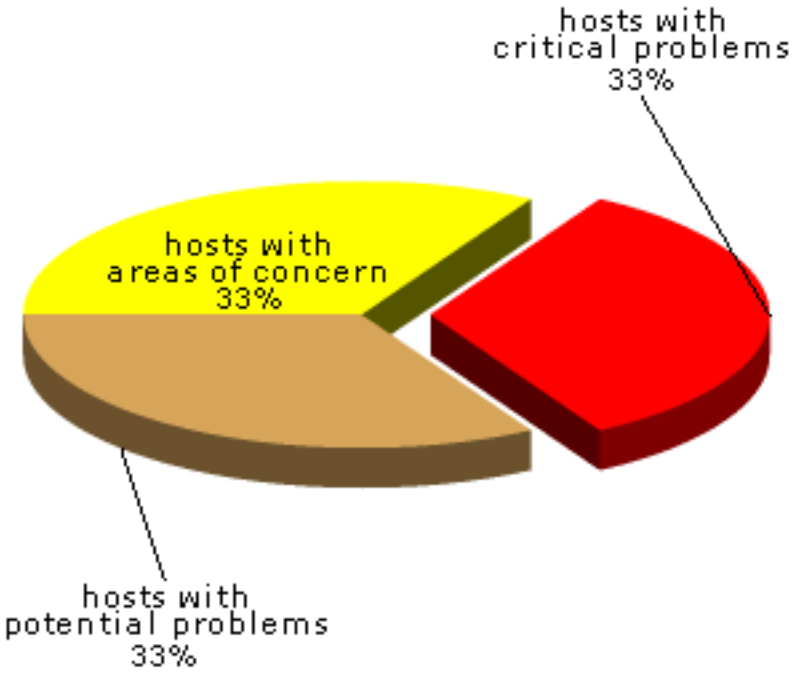




3.2 Hosts by Severity

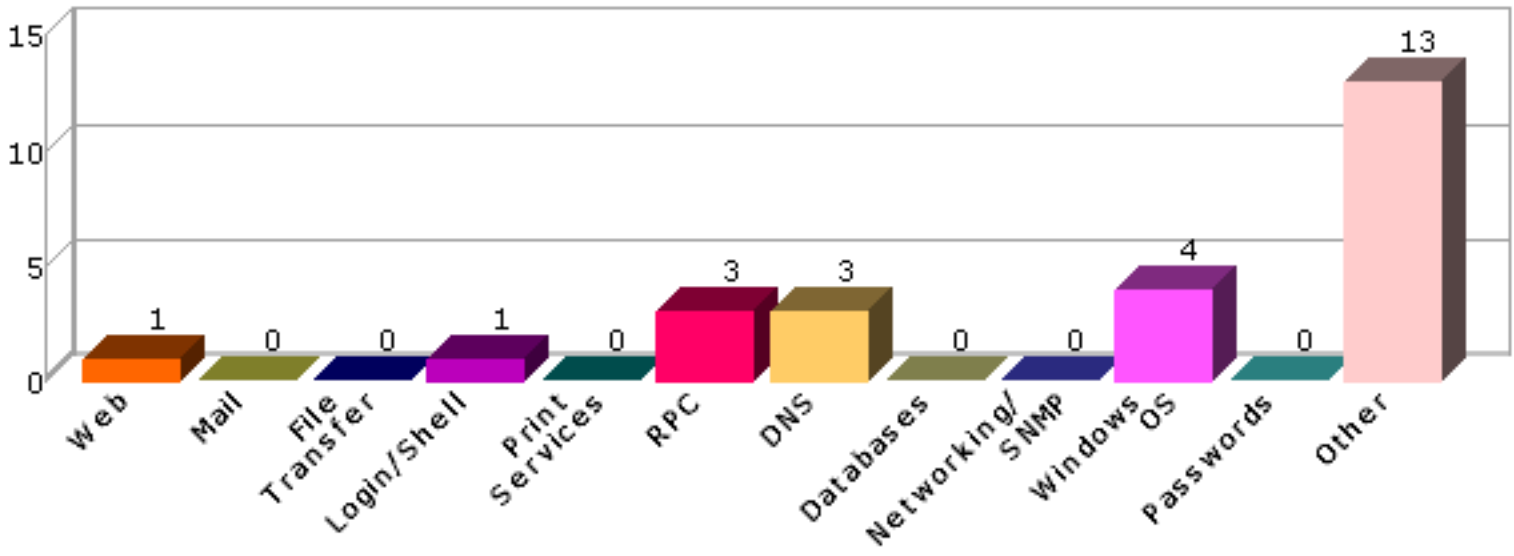
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

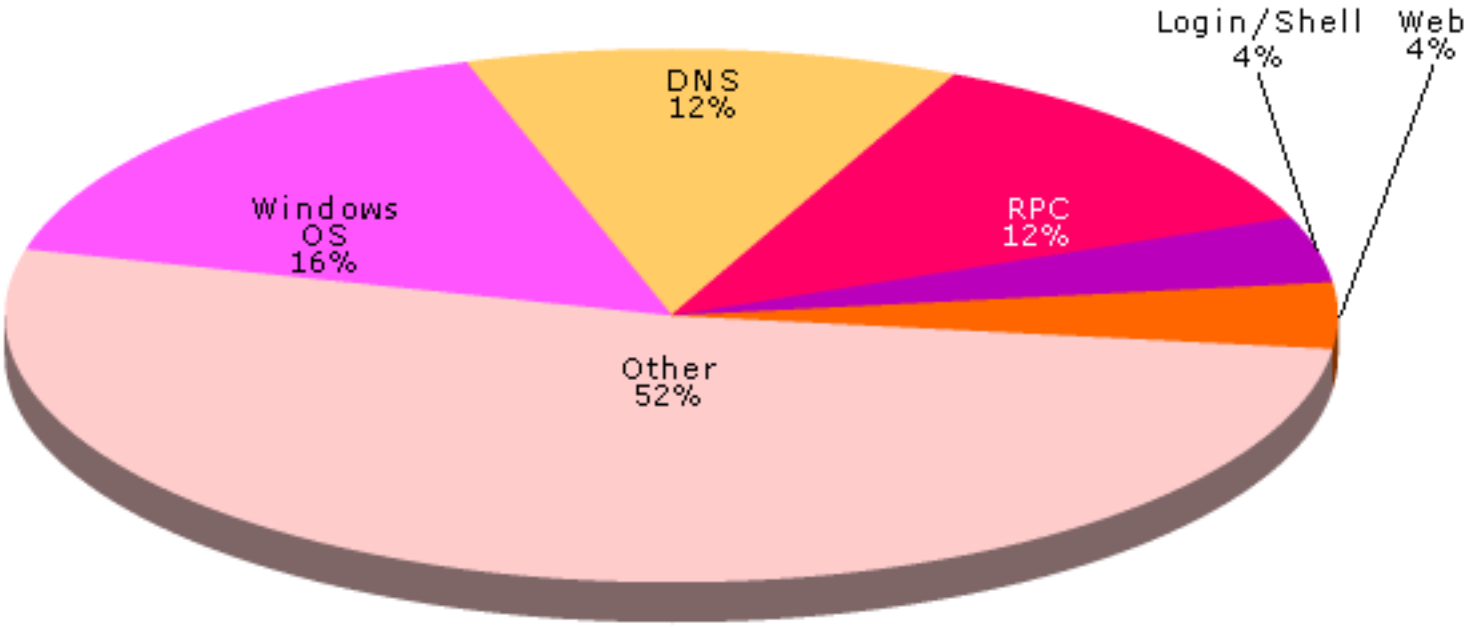




3.3 Vulnerabilities by Class

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





4 Overview

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

4.1 Host List

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

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
saintlab02.sainttest.local		10.8.0.2	Cisco IOS 11.3	0	0	4
xpprounpatched.sainttest.local	XPPROUNPATCHED	10.8.0.14	Windows 2000 SP4	1	0	5
win-iqf3u12cja5.sainttest.local	WIN-IQF3U12CJA5	10.8.0.150	Windows Server 2008 R2	0	2	13

4.2 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
saintlab02.sainttest.local		potential	ICMP timestamp requests enabled	Other	CVE-1999-0524	0.0
saintlab02.sainttest.local	80/tcp	potential	web server uses cleartext HTTP Basic authentication (/)	Web		2.6
saintlab02.sainttest.local	80/tcp	potential	Remote OS available	Other		2.6
saintlab02.sainttest.local	23/tcp	potential	telnet receives cleartext passwords	Login /Shell		2.6
saintlab02.sainttest.local	23/tcp	service	Telnet			
saintlab02.sainttest.local	80/tcp	service	WWW			
saintlab02.sainttest.local	67 /udp	service	bootps (67/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	445 /tcp	potential	scan may have been dynamically blocked by an IPS	Other		2.6
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	445 /tcp	service	microsoft-ds (445/TCP)			
xpprounpatched.sainttest.local	445 /udp	service	microsoft-ds (445/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	1606 /udp	service	slm-api (1606/UDP)			
xpprounpatched.sainttest.local	1900 /udp	service	ssdp (1900/UDP)			
xpprounpatched.sainttest.local	1607 /udp	service	stt (1607/UDP)			
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	1030 /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	1026 /tcp	service	1026/TCP			
win-iqf3u12cja5.sainttest.local	1027 /tcp	service	1027/TCP			
win-iqf3u12cja5.sainttest.local	1029 /tcp	service	1029/TCP			
win-iqf3u12cja5.sainttest.local	1033 /tcp	service	1033/TCP			
win-iqf3u12cja5.sainttest.local	1039 /tcp	service	1039/TCP			
win-iqf3u12cja5.sainttest.local	1044 /tcp	service	1044/TCP			
win-iqf3u12cja5.sainttest.local	9389 /tcp	service	9389/TCP			
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	5985 /tcp	service	WWW (non-standard port 5985)			
win-iqf3u12cja5.sainttest.local	8059 /tcp	service	WWW (non-standard port 8059)			
win-iqf3u12cja5.sainttest.local	8082 /tcp	service	WWW (non-standard port 8082)			
win-iqf3u12cja5.sainttest.local	1025 /tcp	service	blackjack (1025/TCP)			
win-iqf3u12cja5.sainttest.local	1050 /tcp	service	cma (1050/TCP)			
win-iqf3u12cja5.sainttest.local	53 /udp	service	domain (53/UDP)			
win-iqf3u12cja5.sainttest.local	135 /tcp	service	epmap (135/TCP)			
win-iqf3u12cja5.sainttest.local	593 /tcp	service	http-rpc-epmap (593/TCP)			
win-iqf3u12cja5.sainttest.local	1030 /tcp	service	iad1 (1030/TCP)			
win-iqf3u12cja5.sainttest.local	1031 /tcp	service	iad2 (1031/TCP)			
win-iqf3u12cja5.sainttest.local	3260 /tcp	service	iscsi-target (3260/TCP)			
win-iqf3u12cja5.sainttest.local	88/tcp	service	kerberos (88/TCP)			
win-iqf3u12cja5.sainttest.local	464 /tcp	service	kpasswd (464/TCP)			
win-iqf3u12cja5.sainttest.local	389 /tcp	service	ldap (389/TCP)			
win-iqf3u12cja5.sainttest.local	4345 /tcp	service	m4-network-as (4345/TCP)			
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	1047 /tcp	service	neod1 (1047/TCP)
win-iqf3u12cja5.sainttest.local	1048 /tcp	service	neod2 (1048/TCP)
win-iqf3u12cja5.sainttest.local	137 /udp	service	netbios-ns (137/UDP)
win-iqf3u12cja5.sainttest.local	1092 /tcp	service	obrpd (1092/TCP)
win-iqf3u12cja5.sainttest.local	1093 /tcp	service	proofd (1093/TCP)
win-iqf3u12cja5.sainttest.local	2049 /tcp	service	shilp (2049/TCP)
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	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)

5 Details

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

5.1 saintlab02.sainttest.local

IP Address: 10.8.0.2 **Host type:** Cisco IOS 11.3
Scan time: Dec 14 13:08:47 2015

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=807b4296

web server uses cleartext HTTP Basic authentication (*/*)

Severity: Potential Problem

Impact

Poor authentication practices may leave the web application vulnerable to authentication attacks.

Resolution

To use HTML form-based authentication more securely in web applications, do the following:

- Remove the **`value`** attribute from the **`INPUT`** tag corresponding to the password field.
- Submit all forms to an SSL-enabled (*https*) service using the form's **`action`** attribute.
- Place all protected web directories on an SSL-enabled (*https*) service.
- Use the **`autocomplete="off"`** attribute in the **`INPUT`** tag corresponding to the password field.
- Use the **`POST`** method to submit forms containing passwords.

Where can I read more about this?

Additional information on the INPUT element is in the HTML 4.01 Specification, Section 17.4.

For more information on HTTPS, see whatis.com.

For more information on the autocomplete feature in HTML, see HTML Code Tutorial.

Technical Details

Service: http
Received:
WWW-Authenticate: Basic realm="level_15_access"

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

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

Telnet

Severity: Service

Technical Details

WWW

Severity: Service

Technical Details

HTTP/1.1 401 Unauthorized
Date: Mon, 19 Jul 1993 02:09:38 GMT
Server: cisco-IOS
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15_access"
401

bootps (67/UDP)

Severity: Service

Technical Details

5.2 xprounpatched.sainttest.local

IP Address: 10.8.0.14
Scan time: Dec 14 13:08:47 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	KB2621440 and KB2621402 **XP:** 32-bit, 64-bit	12-020

	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)	**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)

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=ef09db03

scan may have been dynamically blocked by an IPS

Severity: Potential Problem

Impact

The scan results may be inconclusive.

Resolution

Temporarily disable the Intrusion Prevention System or configure an exception for the scanner's IP address before starting the scan.

Where can I read more about this?

See pages 14-15 of the PCI DSS ASV Program Guide for more information on handling interference from an IPS during compliance scanning.

Technical Details

Service: 445:TCP
port became closed during scan

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: Mon, 14 Dec 2015 17:51:38 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

microsoft-ds (445/TCP)

Severity: Service

Technical Details

microsoft-ds (445/UDP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

slm-api (1606/UDP)

Severity: Service

Technical Details

ssdp (1900/UDP)

Severity: Service

Technical Details

stt (1607/UDP)

Severity: Service

Technical Details

5.3 win-iqf3u12cja5.sainttest.local

IP Address: 10.8.0.150
Scan time: Dec 14 13:08:47 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. 4888 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
```

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=d013e603

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: iad1
timestamp=43287649; uptime guess=5d 1h 27m 28s

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 17:51:38 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 17:51:42 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 17:51:43 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 17:51:43 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

iscsi-target (3260/TCP)

Severity: Service

Technical Details

kerberos (88/TCP)

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-ns (137/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

unicall (4343/TCP)

Severity: Service

Technical Details