Audit Report

rodrigo ferrer

Audited on May 18, 2023

Reported on May 18, 2023

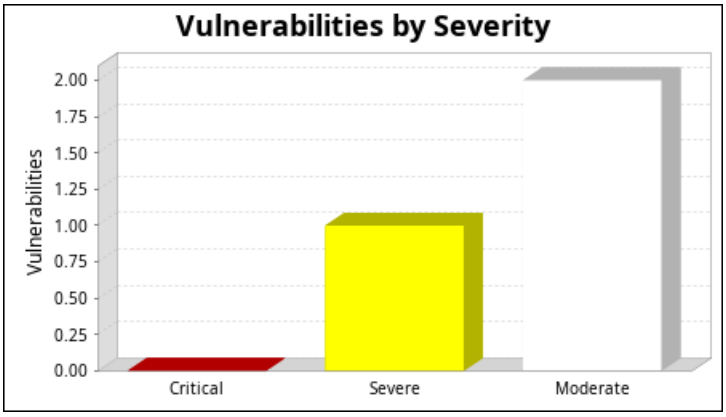
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

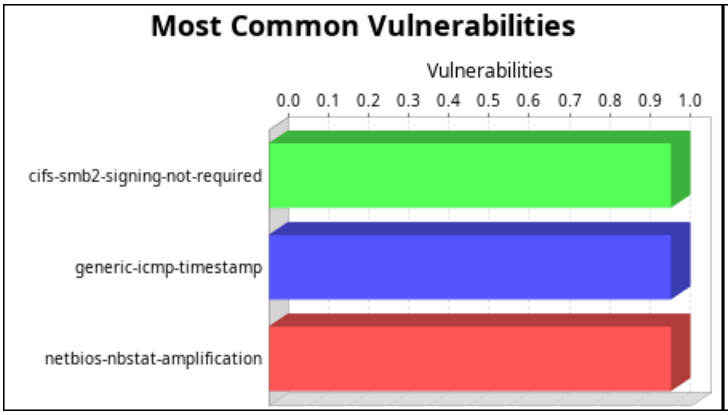
Site Name	Start Time	End Time	Total Time	Status
rodrigo ferrer	May 18, 2023 16:54, COT	May 18, 2023 16:56, COT	1 minutes	Success

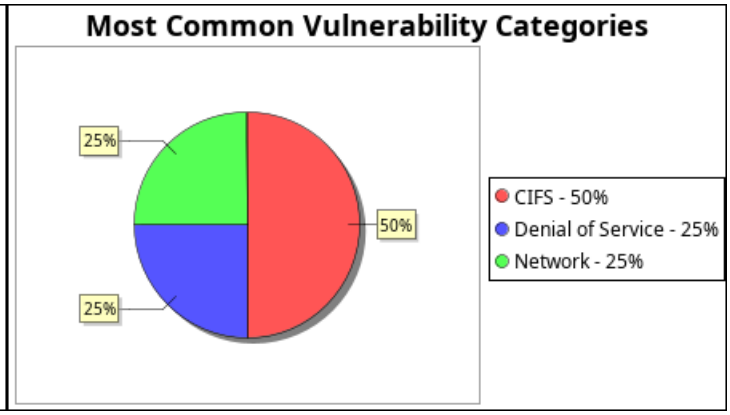
There is not enough historical data to display risk trend.

The audit was performed on one system which was found to be active and was scanned.

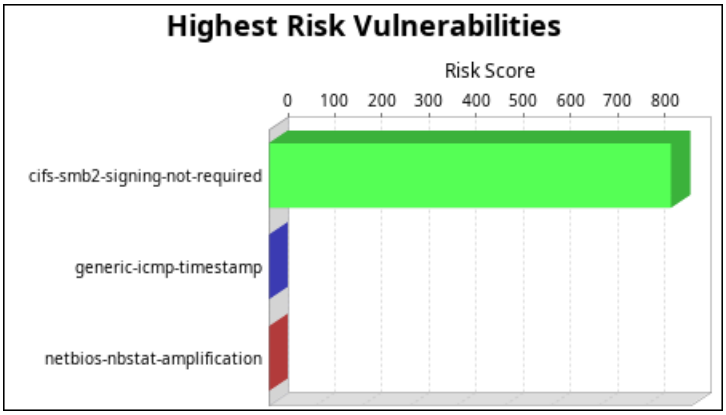


There were 3 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. One vulnerability was severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 2 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.

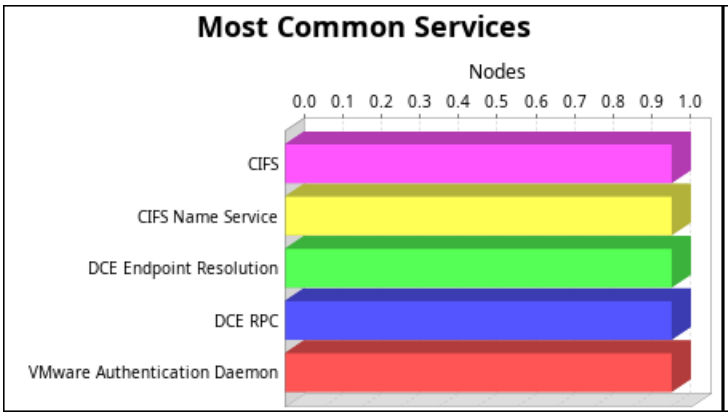


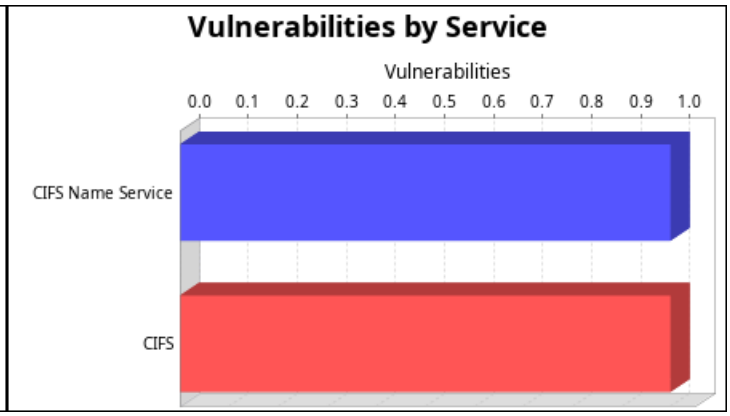


There were 1 occurrences of the cifs-smb2-signing-not-required, generic-icmp-timestamp and netbios-nbstat-amplification vulnerabilities, making them the most common vulnerabilities. There were 2 vulnerability instances in the CIFS category, making it the most common vulnerability category.



The cifs-smb2-signing-not-required vulnerability poses the highest risk to the organization with a risk score of 853. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.
There were 5 services found to be running during this scan.





The CIFS, CIFS Name Service, DCE Endpoint Resolution, DCE RPC and VMware Authentication Daemon services were found on 1 systems, making them the most common services. The CIFS Name Service and CIFS services were found to have the most vulnerabilities during this scan, each with one vulnerability.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.0.11	Microsoft Windows 10	853	•DESKTOP-TSMJQ6U

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

No critical vulnerabilities were reported.

3.2. Severe Vulnerabilities

3.2.1. SMBv2 signing not required (cifs-smb2-signing-not-required)

Description:

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB 2.x signing can be configured in one of two ways: not required (least secure) and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.11:445	Running CIFS serviceConfiguration item smb2-enabled set to 'true' matched Configuration item smb2-signing set to 'enabled' matched

References:

Source	Reference
URL	https://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing for Windows

Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see this Microsoft article for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing for Samba

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

server signing = auto

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

server signing = mandatory

3.3. Moderate Vulnerabilities

3.3.1. ICMP timestamp response (generic-icmp-timestamp)

Description:

ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.11	Able to determine remote system time.

References:

Source	Reference
CVE	CVE-1999-0524
OSVDB	95
XF	306
XF	322

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

deny icmp any any 13

deny icmp any any 14

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

permit icmp any any unreachable

permit icmp any any echo-reply

permit icmp any any time-exceeded
permit icmp any any source-quench

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

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

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

sysctl -w net.inet.icmp.tstamprepl=0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

icmp deny any 13 <inside>

icmp deny any 14 <inside>

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.
The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0

/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.
The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable ICMP timestamp responses on Windows XP/2K3

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.

1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.

11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

Disable ICMP timestamp responses on Windows Vista/2008

ICMP timestamp responses can be disabled via the netsh command line utility.

1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"

For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

•Disable ICMP timestamp responses

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.2. NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)

Description:

A NetBIOS NBSTAT query will obtain the status from a NetBIOS-speaking endpoint, which will include any names that the endpoint is known to respond to as well as the device's MAC address for that endpoint. A NBSTAT response is roughly 3x the size of the request, and because NetBIOS utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.11:137	Running CIFS Name Service serviceConfiguration item advertised-name-count

Affected Nodes:	Additional Information:
	set to '3' matched

References:

Source	Reference
CERT	TA14-017A

Vulnerability Solution:

NetBIOS can be important to the proper functioning of a Windows network depending on the design. Restrict access to the NetBIOS service to only trusted assets.

4. Discovered Services

4.1. CIFS

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	tcp	139	0	
192.168.0.11	tcp	445	1	•smb2-enabled: true •smb2-signing: enabled

4.2. CIFS Name Service

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes. This service is used to handle CIFS browsing (name) requests. Responses contain the names and types of services that can be accessed via CIFS named pipes.

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	udp	137	1	•advertised-name-1: DESKTOP-TSMJQ6U (File Server Service) •advertised-name-2: DESKTOP-TSMJQ6U (Computer Name) •advertised-name-3: WORKGROUP (Domain Name) •advertised-name-count: 3 •mac-address: 9C7BEF154422

4.3. DCE Endpoint Resolution

The DCE Endpoint Resolution service, aka Endpoint Mapper, is used on Microsoft Windows systems by Remote Procedure Call (RPC) clients to determine the appropriate port number to connect to for a particular RPC service. This is similar to the portmapper service used on Unix systems.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	tcp	135	0	

4.4. DCE RPC

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	tcp	49664	0	•interface-uuid: 8FB74744-B2FF-4C00-BE0D-9EF9A191FE1B •interface-version: 1 •name: Ngc Pop Key Service •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49664]
192.168.0.11	tcp	49665	0	•interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •interface-version: 1 •name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D •object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49665]
192.168.0.11	tcp	49666	0	•interface-uuid: F6BEAFF7-1E19-4FBB-9F8F-B89E2018337C •interface-version: 1 •name: Event log TCPIP •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49666]
192.168.0.11	tcp	49667	0	•interface-uuid: 3A9EF155-691D-4449-8D05-09AD57031823 •interface-version: 1 •name: 3A9EF155-691D-4449-8D05-09AD57031823 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49667]
192.168.0.11	tcp	49668	0	•interface-uuid: 29770A8F-829B-4158-90A2-78CD488501F7

Device	Protocol	Port	Vulnerabilities	Additional Information
				•interface-version: 1 •name: 29770A8F-829B-4158-90A2-78CD488501F7 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49668]
192.168.0.11	tcp	49682	0	•interface-uuid: 76F03F96-CDFD-44FC-A22C-64950A001209 •interface-version: 1 •name: 76F03F96-CDFD-44FC-A22C-64950A001209 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49682]
192.168.0.11	tcp	49684	0	•interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 •interface-version: 2 •name: 367ABB81-9844-35F1-AD32-98F038001003 •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49684]
192.168.0.11	tcp	49686	0	•interface-uuid: 6B5BDD1E-528C-422C-AF8C-A4079BE4FE48 •interface-version: 1 •name: Remote Fw APIs •port.discovered.from: tcp/135 •protocol-sequence: ncacn_ip_tcp:192.168.0.11[49686]

4.5. VMware Authentication Daemon

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	tcp	902	0	•VMware Authentication Daemon 1.10 •daemon.protocol: SOAP •display.protocol: VNC •encryption: SSL

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.11	tcp	912	0	•VMware Authentication Daemon 1.0 •daemon.protocol: SOAP •display.protocol: VNC •encryption: None

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.