Audit Report

My Laptop

Audited on December 29, 2022

Reported on December 29, 2022

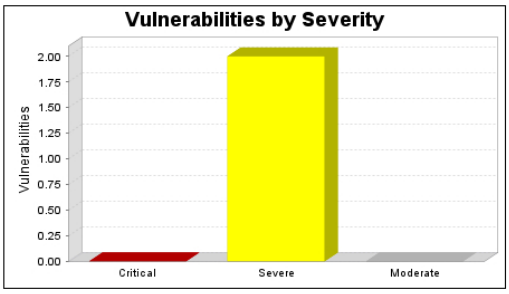
1 EXECUTIVE SUMMARY

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.

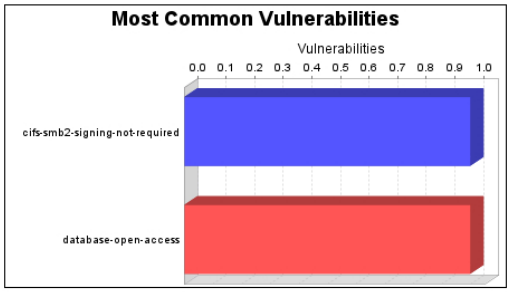
Site Name	Start Time	End Time	Total Time	Status
My Lap	December 29, 2022 19:50, JST	December 29, 2022 19:59, JST	8 minutes	Success

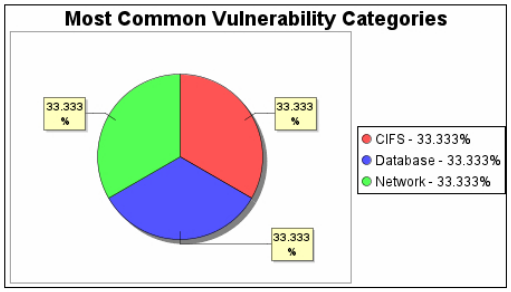
There is not enough historical data to display risk trend.

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

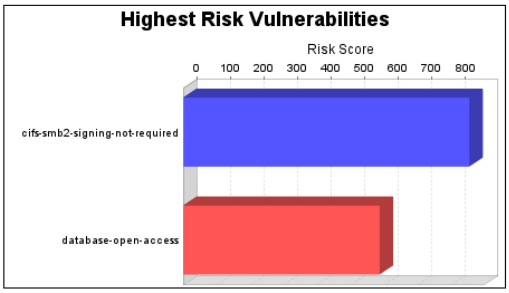


There were 2 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 2 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were no 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.





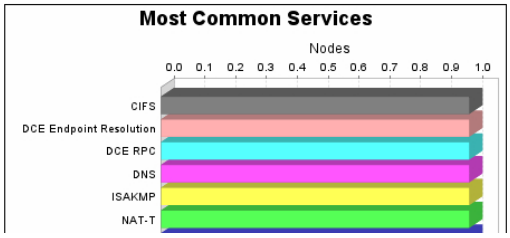
There were 1 occurrences of the cifs-smb2-signing-not-required and database-open-access vulnerabilities, making them the most common vulnerabilities. There were 1 vulnerability instances in the CIFS, Database and Network categories, making them the most common vulnerability categories.

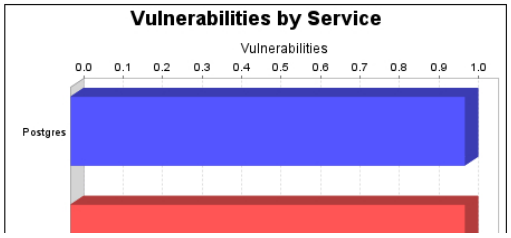


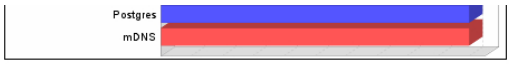
The cifs-smb2-signing-not-required vulnerability poses the highest risk to the organization with a risk score of 852. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

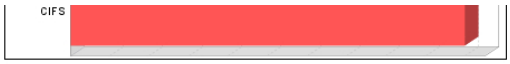
One operating system was identified during this scan.

There were 9 services found to be running during this scan.









The CIFS, DCE Endpoint Resolution, DCE RPC, DNS, ISAKMP, NAT-T, Postgres and mDNS services were found on 1 systems, making them the most common services. The Postgres 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
127.0.0.1	Unknown	1,437	21AK22-12102019 proj_news.xyz

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:
127.0.0.1:445	• Running CIFS service • Configuration 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
  ```

3.2.2 Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.6 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
127.0.0.1:5432	• Running Postgres service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.3 Moderate Vulnerabilities

No moderate vulnerabilities were reported.

4 DISCOVERED SERVICES

4.1 <unknown>

4.1.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	tcp	1001	0	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false tlsv1_3: false
127.0.0.1	udp	1900	0	

4.2 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.

4.2.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	tcp	445	1	smb2-enabled: true smb2-signing: enabled

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
127.0.0.1	tcp	135	0	

4.4 DCE RPC

4.4.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	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:127.0.0.1[49664]
127.0.0.1	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:127.0.0.1[49665]
127.0.0.1	tcp	49666	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:127.0.0.1[49666]
127.0.0.1	tcp	49667	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:127.0.0.1[49667]
127.0.0.1	tcp	55505	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:127.0.0.1[55505]
127.0.0.1	tcp	55506	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:127.0.0.1[55506]
127.0.0.1	tcp	55907	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:127.0.0.1[55907]

4.5 DNS

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser.

4.5.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	udp	53	0	

4.6 ISAKMP

ISAKMP, the Internet Security Association and Key Management Protocol, is used to negotiate and manage security associations for protocols. IKE, the Internet Key Exchange protocol, combines the ISAKMP, Oakley and SKEME protocols to negotiate key exchanges. IPSec, the IP Security protocol uses IKE and ISAKMP to negotiate the encryption and authentication mechanisms to be used.

4.6.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	udp	500	0	

4.7 NAT-T

4.7.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	udp	4500	0	

4.8 Postgres

4.8.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	tcp	5432	1	sslv3: false tlsv1_0: false tlsv1_1: false tlsv1_2: false tlsv1_3: false

4.9 mDNS

4.9.1 Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
127.0.0.1	udp	5353	0	

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.