Nessus Scan Details:

Create scans for VM using 10.0.2.10 (Vulnerable VM)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerabilities Found** | | | | |
| **Vulnerability:** | **CVE Reference:** | **Risk Information:** | **Vulnerability Information:** | **Exploited By:** |
| NFS |  | Risk Factor: Critical  Base Score: 10 | Exploit Available  Publish Date Jan 1st 1985 | Metasploit (NFSMount Scanner) |
| Samba | CVE-2021-44141, CVE-2021-44142, CVE-2022-0336 | Risk Factor: high  Base Score: 8.8 | No known exploits are available  Vulnerability Pub Date: January 31, 2022 |  |
| NFS Shares World Readable |  | RiskFactor: Medium  Base Score: 7.5 | Published: October 26, 2009  Modified: May 5, 2020 | shares without restricting access |
|  |  | Risk Factor: high  Base Score: 8.8 |  |  |
|  |  | Risk Factor: high  Base Score: 8.8 |  |  |
|  |  | Risk Factor: high  Base Score: 8.8 |  |  |

**NFS Exported Share Information Disclosure:**

**Description**

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

The following NFS shares could be mounted :

+ /

+ Contents of / :

- .

- ..

- bin

- boot

- cdrom

- dev

- etc

- home

- initrd.img

- lib

- lib64

- lost+found

- media

- mnt

- opt

- proc

- root

- run

- sbin

- srv

- sys

- tmp

- usr

- var

- vmlinuz

**Plugin Details**

Severity: Critical

ID: 11356

Version: 1.20

Type: remote

Family: RPC

Published: March 12, 2003

Modified: September 17, 2018

**SAMBA**

**Description**

The version of Samba running on the remote host is 4.13.x prior to 4.13.17, 4.14.x prior to 4.14.12, or 4.15.x prior to 4.15.5. It is, therefore, affected by multiple vulnerabilities:

- Out-of-bounds heap read/write vulnerability in VFS module vfs\_fruit allows code execution. (CVE-2021-44142)

- Information leak via symlinks of existence of files or directories outside of the exported share. (CVE-2021-44141)

- Samba AD users with permission to write to an account can impersonate arbitrary services. (CVE-2022-0336)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

**Solution**

Upgrade to Samba version 4.13.17, 4.14.12, or 4.15.5 or later.

**See Also**

https://www.samba.org/samba/history/security.html

https://www.samba.org/samba/security/CVE-2021-44141.html

https://www.samba.org/samba/security/CVE-2021-44142.html

https://www.samba.org/samba/security/CVE-2022-0336.html

**Output**

Installed version : 4.3.11-Ubuntu

Fixed version : 4.13.17

**plugin Details**

Severity: High

ID: 157360

Version: 1.4

Type: remote

Family: Misc.

Published: February 3, 2022

Modified: April 5, 2022

**Risk Information**

Risk Factor: High

CVSS v3.0 Base Score 8.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.7

CVSS v2.0 Base Score: 9.0

CVSS v2.0 Temporal Score: 6.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

**Vulnerability Information**

CPE: cpe:/a:samba:samba

Exploit Ease: No known exploits are available

Patch Pub Date: January 31, 2022

Vulnerability Pub Date: January 31, 2022

**Reference Information**

IAVA: 2022-A-0054

CVE: CVE-2021-44141, CVE-2021-44142, CVE-2022-0336

**NFS Shares World Readable**

**Description**

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

**Solution**

Place the appropriate restrictions on all NFS shares.

**See Also**

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

**Output**

The following shares have no access restrictions :

/ \*

/home \*

**Plugin Details**

Severity: High

ID: 42256

Version: 1.11

Type: remote

Family: RPC

Published: October 26, 2009

Modified: May 5, 2020

**Risk Information**

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

**Vulnerability Information**

Vulnerability Pub Date: January 1, 1985

**My Host Discovery Scan / Plugin #19506**

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.

- The type of scanner (Nessus or Nessus Home).

- The version of the Nessus Engine.

- The port scanner(s) used.

- The port range scanned.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- The date of the scan.

- The duration of the scan.

- The number of hosts scanned in parallel.

- The number of checks done in parallel.

Output

Information about this scan :

Nessus version : 10.1.2

Nessus build : 20068

Plugin feed version : 202204130945

Scanner edition used : Nessus Home

Scanner OS : LINUX

Scanner distribution : debian6-x86-64

Scan type : Normal

Scan name : My Host Discovery Scan

Scan policy used : Host Discovery

Scanner IP : 10.0.2.15

WARNING : No port scanner was enabled during the scan. This may

lead to incomplete results.

Port range : default

Ping RTT : 245.442 ms

Thorough tests : no

Experimental tests : no

Paranoia level : 1

Report verbosity : 1

Safe checks : yes

Optimize the test : yes

Credentialed checks : no

Patch management checks : None

Display superseded patches : yes (supersedence plugin launched)

CGI scanning : disabled

Web application tests : disabled

Max hosts : 256

Max checks : 5

Recv timeout : 5

Backports : None

Allow post-scan editing: Yes

Scan Start Date : 2022/4/13 12:16 EDT

Scan duration : 7 sec

Export

**My Host Discovery Scan / Plugin #10180**

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Output

The remote host is up

The host replied to an ARP who-is query.

Hardware address : 08:00:27:88:41:6d