ScanNet1

Report generated by Tenable Nessus™ Thu, 29 May 2025 08:59:46 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.3.9

1	1	0	1	63
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu May 29 08:44:52 2025
End time: Thu May 29 08:59:46 2025

Host Information

IP: 10.0.3.9
MAC Address: 08:00:27:2B:3F:BB
OS: Linux Kernel 6.1.135-1.el9.elrepo.x86_64 on AlmaLinux release 9.5 (Teal Serval)

Vulnerabilities

236860 - AlmaLinux 9 : firefox (ALSA-2025:4443)

Synopsis

The remote AlmaLinux host is missing one or more security updates.

Description

The remote AlmaLinux 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the ALSA-2025:4443 advisory.

* firefox: thunderbird: Privilege escalation in Firefox Updater (CVE-2025-2817)

* firefox: thunderbird: Unsafe attribute access during XPath parsing (CVE-2025-4087)

* firefox: thunderbird: Process isolation bypass using javascript: URI links in cross-origin frames (CVE-2025-4083)

* firefox: thunderbird: Memory safety bugs fixed in Firefox 138, Thunderbird 138, Firefox ESR 128.10, and Thunderbird 128.10 (CVE-2025-4091)

* firefox: thunderbird: Memory safety bug fixed in Firefox ESR 128.10 and Thunderbird 128.10 (CVE-2025-4093)

Tenable has extracted the preceding description block directly from the AlmaLinux security advisory.

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

See Also

https://errata.almalinux.org/9/ALSA-2025-4443.html
https://access.redhat.com/errata/RHSA-2025:4443

Solution

Update the affected firefox and / or firefox-x11 packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2025-2817
CVE	CVE-2025-4083
CVE	CVE-2025-4087
CVE	CVE-2025-4091
CVE	CVE-2025-4093
XREF	ALSA:2025:4443
XREF	RHSA:2025:4443
XREF	CWE:120
XREF	CWE:125
XREF	CWE:653

XREF CWE:94

Plugin Information

Published: 2025/05/16, Modified: 2025/05/16

Plugin Output

tcp/0

```
Remote package installed : firefox-128.9.0-2.el9_5
Should be                : firefox-128.10.0-1.el9_5.alma.1
```

235711 - AlmaLinux 9 : emacs (ALSA-2025:4787)

Synopsis

The remote AlmaLinux host is missing a security update.

Description

The remote AlmaLinux 9 host has packages installed that are affected by a vulnerability as referenced in the ALSA-2025:4787 advisory.

* emacs: arbitrary code execution via Lisp macro expansion (CVE-2024-53920)

Tenable has extracted the preceding description block directly from the AlmaLinux security advisory.

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

See Also

https://errata.almalinux.org/9/ALSA-2025-4787.html

https://access.redhat.com/errata/RHSA-2025:4787

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-53920
XREF	ALSA:2025:4787
XREF	RHSA:2025:4787
XREF	CWE:94

Plugin Information

Published: 2025/05/12, Modified: 2025/05/12

Plugin Output

tcp/0

```
Remote package installed : emacs-filesystem-27.2-11.el9_5.1
Should be                : emacs-filesystem-27.2-11.el9_5.2
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.0037

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : 1.2
Vendor       : innotek GmbH
Release Date : 12/01/2006
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/04/15

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:almalinux:almalinux:9.5::~~~~x86_64~ -> AlmaLinux

Following application CPE's matched on the remote system :

  cpe:/a:exiv2:exiv2:0.27.5 -> Exiv2
  cpe:/a:exiv2:libexiv2:0.27.5
  cpe:/a:gnome:gnome-shell:40.10 -> GNOME gnome-shell -
  cpe:/a:gnupg:libgcrypt:1.10.0 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.76.1 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.76.1 -> Haxx libcurl
  cpe:/a:openbsd:openssh:8.7 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:3.2.2 -> OpenSSL Project OpenSSL
  cpe:/a:podman_project:podman:5.2.2 -> Podman Project Podman
  cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
  cpe:/a:vim:vim:8.2 -> Vim
```

```
cpe:/a:vmware:open_vm_tools:12.4.0 -> VMware Open VM Tools
```

182774 - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path              : /usr/bin/curl
Version           : 7.76.1
Associated Package : curl-7.76.1-31.el9
Managed by OS     : True
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/04/28

Plugin Output

tcp/0

```
Hostname : localhost.localdomain
  localhost.localdomain (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 10.0.3.9 (on interface enp0s3)
 - 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - fe80::a00:27ff:fe2b:3fbb (on interface enp0s3)
 - ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

  - 08:00:27:2b:3f:bb (interface enp0s3)
```

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
        ScopeID : 0x10
enp0s3:
  MAC : 08:00:27:2b:3f:bb
  IPv4:
    - Address : 10.0.3.9
        Netmask : 255.255.255.0
        Broadcast : 10.0.3.255
  IPv6:
    - Address : fe80::a00:27ff:fe2b:3fbb
        Prefixlen : 64
        Scope : link
        ScopeID : 0x20
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  enp0s3:
    ipv4_gateways:
      10.0.3.1:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  enp0s3:
    ipv4_subnets:
     - 10.0.3.0/24
    ipv6_subnets:
     - fe80::/64
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/04/30

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/sbin
/bin
/usr/sbin
/usr/bin
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:2B:3F:BB : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/04/28

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:2B:3F:BB
```

204827 - Exiv2 Installed (Linux / Unix)

Synopsis

Exiv2 is installed on the remote Linux / Unix host.

Description

Exiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204827' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path              : /usr/bin/exiv2
Version           : 0.27.5
Associated Package : exiv2-0.27.5-2.el9
Managed by OS     : True
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 3.0.5)
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/04/28

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ enp0s3
  + IPv4
    - Address       : 10.0.3.9
      Assign Method : static
  + IPv6
    - Address       : fe80::a00:27ff:fe2b:3fbb
      Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/04/30

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /usr/lib64/libgcrypt.so.20
  Version : 1.10.0

  Path    : /usr/lib64/libgcrypt.so.20.4.0
  Version : 1.10.0
```

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem                  Size  Used Avail Use% Mounted on
devtmpfs                    4.0M     0  4.0M   0% /dev
tmpfs                       884M     0  884M   0% /dev/shm
tmpfs                       354M  9.6M  344M   3% /run
/dev/mapper/almalinux-root   32G  7.3G   24G  24% /
/dev/sda1                   960M  561M  400M  59% /boot
tmpfs                       177M   56K  177M   1% /run/user/42
tmpfs                       177M   40K  177M   1% /run/user/1000
tmpfs                       177M   40K  177M   1% /run/user/1001


$ lsblk
NAME               MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda                  8:0    0 34.2G  0 disk
|-sda1               8:1    0    1G  0 part /boot
`-sda2               8:2    0 33.2G  0 part
  |-almalinux-root 253:0    0 31.2G  0 lvm  /
  `-almalinux-swap 253:1    0    2G  0 lvm  [SWAP]
sr0                 11:0    1   51M  0 rom


$ mount -l
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
```

```
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=4096k,nr_inodes=217990,mode=755,inode64)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,seclabel,size=361772k,nr_inodes=819200,mode=755,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2
 (rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime,seclabel)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
/dev/mapper/almalinux-root on / type xfs
 (rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
selinuxfs on /sys/fs/selinux type selinuxfs (rw,nosuid,noexec,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
 (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=18735)
debug [...]
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: CEST +0200
Via timedatectl: Time zone: Europe/Warsaw (CEST, +0200)
Via /etc/localtime: CET-1CEST,M3.5.0,M10.5.0/3
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

```
----------[ User Accounts ]-----------

User         : alma
Home folder  : /home/alma
Start script : /bin/bash
Groups       : alma
               wheel

User         : tenacc
Home folder  : /home/tenacc
Start script : /bin/bash
Groups       : tenacc
               wheel

----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

User         : bin
Home folder  : /bin
Start script : /sbin/nologin
Groups       : bin

User         : daemon
Home folder  : /sbin
Start script : /sbin/nologin
```

```
Groups       : daemon

User         : adm
Home folder  : /var/adm
Start script : /sbin/nologin
Groups       : adm

User         : lp
Home folder  : /var/spool/lpd
Start script : /sbin/nologin
Groups       : lp

User         : sync
Home folder  : /sbin
Start script : /bin/sync
Groups       : root

User         : shutdown
Home folder  : /sbin
Start script : /sbin/shutdown
Groups       : root

User         : halt
Home folder  : /sbin
Start script : /sbin/halt
Groups       : root

User         : mail
Home folder  : /var/spool/mail
Start script : /sbin/nologin
Groups       : mail

User         : operator
Home folder  : /root
Start script : /sbin/nologin
Groups       : root

User         : games
Home folder  : /usr/games
Start script : /sbin/nologin
Groups       : users

User         : ftp
Home folder  : /var/ftp
Start script : /sbin/nologin
Groups       : ftp

User         : nobody
Home folder  : /
Start script : /sbin/nologin
Groups       : nobody

User         : tss
Home folder  : /
Start script : /usr/sbin/nologin
Groups       : tss

User         : systemd-coredump
Home folder  : /
Start script : /sbin/nologin
Groups       : systemd-coredump

User         : dbus
Home folder  : /
Start script : /sbin/nologin
Groups       : dbus

User         : polkitd
Home folder  : /
Start script : /sbin/nologin
```

```
Groups       : polkitd

User         : avahi
Home folder  : /var/run/avahi-daemon
Start script : /sbin/nologin
Groups       : avahi

User         : geoclue
Home folder  : / [...]
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202505271020
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : es8-x86-64
Scan type : Normal
Scan name : ScanNet1
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.0.3.15
Port scanner(s) : netstat
Port range : 1-65535
Ping RTT : 104.530 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'tenacc' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/5/29 8:45 EDT (UTC -04:00)
Scan duration : 867 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/5353/mdns

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/33064

```
Port 33064/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/54215

```
Port 54215/udp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 18.04 Linux Kernel 4.15
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 6.1.135-1.el9.elrepo.x86_64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux localhost.localdomain 6.1.135-1.el9.elrepo.x86_64 #1 SMP PREEMPT_DYNAMIC
 Sun Apr 27 03:44:37 EDT 2025 x86_64 x86_64 x86_64 GNU/Linux


Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B10113:F0x12:W64240:O0204ffff:M1460:
   P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191004_7_p=22

Remote operating system : Linux Kernel 6.1.135-1.el9.elrepo.x86_64 on AlmaLinux release 9.5 (Teal
 Serval)
```

```
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 SSH:!:SSH-2.0-OpenSSH_8.7
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/05/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.1.135-1.el9.elrepo.x86_64 on AlmaLinux release 9.5 (Teal
 Serval)
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 6.1.135-1.el9.elrepo.x86_64 on AlmaLinux release 9.5 (Teal
 Serval)
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux localhost.localdomain 6.1.135-1.el9.elrepo.x86_64 #1 SMP PREEMPT_DYNAMIC Sun Apr 27 03:44:37
 EDT 2025 x86_64 x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote AlmaLinux system is :
AlmaLinux release 9.5 (Teal Serval)

OS Security Patch Assessment is available for this host.
Runtime : 21.528323 seconds
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account  : tenacc
Protocol : SSH
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/04/28

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.7
Banner  : SSH-2.0-OpenSSH_8.7
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/04/30

Plugin Output

tcp/0

```
Nessus detected 2 installs of OpenSSL:

  Path               : /usr/lib64/libcrypto.so.3.2.2
  Version            : 3.2.2
  Associated Package : openssl-libs-3.2.2-6.el9_5.1.x86_64

  Path               : /usr/bin/openssl
  Version            : 3.2.2
  Associated Package : openssl-3.2.2-6.el9_5.1
  Managed by OS      : True
```

```
We are unable to retrieve version info from the following list of OpenSSL files. However, these
 installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib64/libssl.so.3.2.2
```

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/05/13

Plugin Output

tcp/0

```
. You need to take the following 2 actions :

[ AlmaLinux 9 : emacs (ALSA-2025:4787) (235711) ]

+ Action to take : Update the affected packages.

[ AlmaLinux 9 : firefox (ALSA-2025:4443) (236860) ]

+ Action to take : Update the affected firefox and / or firefox-x11 packages.
```

233359 - Podman Installed (Linux)

Synopsis

Podman was detected on the remote host.

Description

Podman, a daemonless, open source, Linux native tool designed to make it easy to find, run, build, share and deploy applications using Open Containers Initiative (OCI) Containers and Container Images, is installed on the remote host.

See Also

https://docs.podman.io/en/latest/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/26, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path          : podman-5.2.2-15.el9_5 (via package manager)
Version       : 5.2.2
Managed by OS : True
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519

The server supports the following options for encryption_algorithms_client_to_server :
```

```
  aes128-ctr
  aes128-gcm@openssh.com
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : tenacc
Commands failed due to privilege escalation failure:
- Escalation account : tenacc
  Escalation method  : sudo
  Plugins :
  - Plugin Filename : bios_get_info_ssh.nasl
    Plugin ID       : 34098
    Plugin Name     : BIOS Info (SSH)
    - Command  : "LC_ALL=C dmidecode"
      Response : "# dmidecode 3.6\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\nCan't read memory from /dev/mem"
      Error    : ""
    - Command  : "LC_ALL=C /usr/sbin/dmidecode"
      Response : "# dmidecode 3.6\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\nCan't read memory from /dev/mem"
      Error    : ""
```

```
    - Command  : "LC_ALL=C /sbin/dmidecode"
      Response : "# dmidecode 3.6\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\nCan't read memory from /dev/mem"
      Error    : ""
  - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
    Plugin ID       : 125216
    Plugin Name     : Processor Speculative Execution Vulnerabilities (Linux)
    - Command  : "head /sys/kernel/debug/x86/pti_enabled"
      Response : "head: cannot open '/sys/kernel/debug/x86/pti_enabled' for reading: Permission
 denied"
      Error    : ""
    - Command  : "head /sys/kernel/debug/x86/retp_enabled"
      Response : "head: cannot open '/sys/kernel/debug/x86/retp_enabled' for reading: Permission
 denied"
      Error    : ""
    - Command  : "head /sys/kernel/debug/x86/ibrs_enabled"
      Response : "head: cannot open '/sys/kernel/debug/x86/ibrs_enabled' for reading: Permission
 denied"
      Error    : ""
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.7
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Alma Linux system :

  fonts-filesystem-2.0.5-7.el9.1|1 Tue Apr 29 11:51:30 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  hwdata-0.348-9.15.el9|(none) Tue Apr 29 11:51:30 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  xkeyboard-config-2.33-2.el9|(none) Tue Apr 29 11:51:30 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  liberation-fonts-common-2.1.3-5.el9|1 Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  hyperv-daemons-license-0-0.43.20190303git.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux
 Packaging Team <packager@almalinux.org>
  abattis-cantarell-fonts-0.301-4.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux Packaging
 Team <packager@almalinux.org>
  yelp-xsl-40.2-1.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  mozilla-filesystem-1.9-30.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux Packaging Team
 <packager@almalinux.org>
  google-noto-fonts-common-20201206-4.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux
 Packaging Team <packager@almalinux.org>
  google-noto-cjk-fonts-common-20230817-2.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux
 Packaging Team <packager@almalinux.org>
```

```
 foomatic-db-filesystem-4.0-72.20210209.el9|(none) Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux
Packaging Team <packager@almalinux.org>
 cups-filesystem-2.3.3op2-31.el9_5|1 Tue Apr 29 11:51:32 2025|AlmaLinux|AlmaLinux Packaging Team
<packager@almalinux.org>
 appstream-data-9-20240827.el9|1 Tue Apr 29 11:51:33 2025|AlmaLinux|AlmaLinux Packaging Team
<packager@almalinux.org>
 adobe-mappings-cmap-20171205-12.el9|(none) Tue Apr 29 11:51:33 2025|AlmaLinux|AlmaLinux Packaging
Team <packager@almalinux.org>
 pcre2-syntax-10.40-6.el9|(none) Tue Apr 29 11:51:34 2025|AlmaLinux|AlmaLinux Packaging Team
<packager@almalinux.org>
 libreport-filesystem-2.15.2-6.el9.alma|(none) Tue Apr 29 11:51:34 2025|AlmaLinux| [...]
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User:       'tenacc'
Port:       22
Proto:      SSH
Method:     password
Escalation: sudo


See the output of the following plugin for details :

  Plugin ID   : 102094
  Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User:       'tenacc'
Port:       22
Proto:      SSH
Method:     password
Escalation: sudo
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot   system boot  6.1.135-1.el9.el Thu May 29 14:30   still running
reboot   system boot  6.1.135-1.el9.el Wed May 28 23:16   still running
reboot   system boot  6.1.135-1.el9.el Wed May 28 22:12   still running
reboot   system boot  6.1.135-1.el9.el Wed May 28 20:27   still running
reboot   system boot  6.1.135-1.el9.el Wed May 28 19:35   still running
reboot   system boot  6.1.135-1.el9.el Thu May 15 13:35   still running
reboot   system boot  6.1.135-1.el9.el Tue May 13 10:38   still running
reboot   system boot  6.1.135-1.el9.el Tue May  6 18:21   still running
reboot   system boot  6.1.135-1.el9.el Tue May  6 10:17   still running
reboot   system boot  6.1.135-1.el9.el Mon May  5 21:11   still running
reboot   system boot  6.1.135-1.el9.el Mon May  5 21:02   still running
reboot   system boot  6.1.135-1.el9.el Tue Apr 29 19:43   still running
reboot   system boot  5.14.0-503.38.1. Tue Apr 29 19:28 - 19:43  (00:15)
reboot   system boot  5.14.0-503.38.1. Tue Apr 29 19:20 - 19:27  (00:07)
reboot   system boot  5.14.0-503.11.1. Tue Apr 29 18:11 - 19:20  (01:08)
reboot   system boot  5.14.0-503.11.1. Tue Apr 29 16:39 - 19:20  (02:40)

wtmp begins Tue Apr 29 16:39:23 2025
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.3.15 to 10.0.3.9 :
10.0.3.15
10.0.3.9

Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/04/30

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-5.2.5-8.el9_0.x86_64
  Confidence         : High
```

```
   Version Source     : Package

   Path               : /usr/lib64/liblzma.so.5.2.5
   Version            : 5.2.5
   Associated Package : xz-libs-5.2.5-8.el9_0.x86_64
   Confidence         : High
   Version Source     : Package
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  0.9 109444 17516 ?        Ss   14:29   0:04 /usr/lib/systemd/systemd --
switched-root --system --deserialize 31 rhgb
root           2  0.0  0.0      0     0 ?        S    14:29   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   14:29   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   14:29   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   14:29   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   14:29   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   14:29   0:00 [kworker/0:0H-events_highpri]
root           9  0.1  0.0      0     0 ?        I    14:29   0:01 [kworker/u2:0-writeback]
root          10  0.0  0.0      0     0 ?        I<   14:29   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    14:29   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    14:29   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    14:29   0:00 [rcu_tasks_trace_kthread]
root          14  0.1  0.0      0     0 ?        S    14:29   0:01 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    14:29   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    14:29   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    14:29   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    14:29   0:00 [kdevtmpfs]
root          21  0.0  0.0      0     0 ?        I<   14:29   0:00 [inet_frag_wq]
root          22  0.0  0.0      0     0 ?        S    14:29   0:00 [kauditd]
root          23  0.0  0.0      0     0 ?        S    14:29   0:00 [khungtaskd]
root          24  0.0  0.0      0     0 ?        I    14:29   0:00 [kworker/u2:1-events_unbound]
root          25  0.0  0.0      0     0 ?        S    14:29   0:00 [oom_reaper]
root          26  0.0  0.0      0     0 ?        I<   14:29   0:00 [writeback]
root    [...]
```

152742 - Unix Software Discovery Commands Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Unix software discovery checks are available.

Account  : tenacc
Protocol : SSH
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?c0628155

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path    : /usr/bin/vmtoolsd
Version : 12.4.0
```

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path    : /usr/bin/vim
Version : 8.2
```

198234 - gnome-shell Installed (Linux / UNIX)

Synopsis

gnome-shell is installed on the remote Linux / UNIX host.

Description

gnome-shell is installed on the remote Linux / UNIX host.

See Also

https://gitlab.gnome.org/GNOME/gnome-shell/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2025/04/30

Plugin Output

tcp/0

```
Nessus detected 2 installs of GNOME Shell:

  Path    : /bin/gnome-shell
  Version : 40.10
  Managed : 1

  Path    : /usr/bin/gnome-shell
  Version : 40.10
  Managed : 1
```

138014 - kpatch : Installed Patches

Synopsis

The remote host is using kpatch to maintain the OS kernel.

Description

kpatch is being used to maintain the remote host's operating system kernel without requiring reboots.

See Also

https://github.com/dynup/kpatch

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/07/01, Modified: 2021/05/10

Plugin Output

tcp/0

```
kpatch is installed, but no loaded patch modules appear to cover any CVEs.
kpatch list output:

Loaded patch modules:

Installed patch modules:
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path               : /usr/lib64/libcurl.so.4.7.0
Version            : 7.76.1
Associated Package : libcurl-7.76.1-31.el9
Managed by OS      : True
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/04/30

Plugin Output

tcp/0

```
Path              : /usr/lib64/libexiv2.so.0.27.5
Version           : 0.27.5
Associated Package : exiv2-libs-0.27.5-2.el9
Managed by OS     : True
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : linux.local.
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 3.0.5)
Version : 3.0.5
```