Task3_NessusScan

Report generated by Tenable Nessus™ Mon, 17 Nov 2025 17:25:32 IST

Nessus Essentials

TABLE OF CONTENTS

Vulnerabilities by Host

Nessus Essentials

Nessus Essentials

Vulnerabilities by Host

127.0.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	3	0	41

Host Information

IP: 127.0.0.1

Vulnerabilities

270698 - Ruby RACK < 2.2.20 / 3.x < 3.1.18 / 3.2 < 3.2.3 Multiple Vulnerabilities

Synopsis

The remote host has an application installed that is affected by DoS vulnerability.

Description

The version of the RACK Ruby library installed on the remote host is prior to 2.2.20 / 3.1.18 / 3.2.3. It is, therefore, affected by the following vulnerabilities:

- Rack::Request#POST reads the entire request body into memory for Content-Type: application/x-www-form-urlencoded, calling rack.input.read(nil) without enforcing a length or cap. Large request bodies can therefore be buffered completely into process memory before parsing, leading to denial of service (DoS) through memory exhaustion. (CVE-2025-61919)

- A possible information disclosure vulnerability existed in Rack::Sendfile when running behind a proxy that supports x-sendfile headers (such as Nginx). Specially crafted headers could cause Rack::Sendfile to miscommunicate with the proxy and trigger unintended internal requests, potentially bypassing proxy-level access restrictions. (CVE-2025-61780)

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://github.com/rack/rack/security/advisories/GHSA-r657-rxjc-j557

https://github.com/rack/rack/security/advisories/GHSA-6xw4-3v39-52mm

Solution

Upgrade to RACK version 2.2.20 / 3.1.18 / 3.2.3 or later.

Risk Factor

Nessus Essentials

High

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.0062

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-46727
CVE	CVE-2025-61919
XREF	IAVB:2025-B-0171

Plugin Information

Published: 2025/10/17, Modified: 2025/10/17

Plugin Output

tcp/0

```
Path              : /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rack-3.1.16
Installed version : 3.1.16
Fixed version     : 3.1.18
```

269982 - Ruby Rack < 2.2.19 / 3.1.x < 3.1.17 / 3.2.x < 3.2.2 Multiple Vulnerabilities

Synopsis

The remote host has a Ruby library installed that is affected by multiple vulnerabilities.

Description

The version of the Rack Ruby library installed on the remote host is prior to 2.2.19, 3.1.x prior to 3.1.17, or 3.2.x prior to 3.2.2. It is, therefore, affected by multiple vulnerabilities:

- Rack::Multipart::Parser buffers the entire multipart preamble (bytes before the first boundary) in memory without any size limit. A client can send a large preamble followed by a valid boundary, causing significant memory use and potential process termination due to out-of-memory (OOM) conditions.

(CVE-2025-61770)

- Rack::Multipart::Parser stores non-file form fields (parts without a filename) entirely in memory as Ruby String objects. A single large text field in a multipart/form-data request (hundreds of megabytes or more) can consume equivalent process memory, potentially leading to out-of-memory (OOM) conditions and denial of service (DoS). (CVE-2025-61771)

- Rack::Multipart::Parser can accumulate unbounded data when a multipart part's header block never terminates with the required blank line (CRLFCRLF). The parser keeps appending incoming bytes to memory without a size cap, allowing a remote attacker to exhaust memory and cause a denial of service (DoS).

(CVE-2025-61772)

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://github.com/advisories/GHSA-p543-xpfm-54cp

https://github.com/advisories/GHSA-w9pc-fmgc-vxvw

https://github.com/advisories/GHSA-wpv5-97wm-hp9c

Solution

Upgrade to Rack version 2.2.19, 3.1.17, 3.2.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-61770
CVE	CVE-2025-61771
CVE	CVE-2025-61772
XREF	IAVB:2025-B-0167

Plugin Information

Published: 2025/10/10, Modified: 2025/10/10

Plugin Output

tcp/0

```
Path              : /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rack-3.1.16
Installed version : 3.1.16
Fixed version     : 3.1.17
```

265895 - Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability

Synopsis

The remote host has an application installed that is affected by a DoS vulnerability.

Description

The version of the REXML Ruby library installed on the remote host is 3.3.3 prior to 3.4.2. It is, therefore, affected by a DoS vulnerability as referenced in GHSA-c2f4-jgmc-q2r5 advisory.

- REXML is an XML toolkit for Ruby. The REXML gems from 3.3.3 to 3.4.1 has a DoS vulnerability when parsing XML containing multiple XML declarations. If you need to parse untrusted XMLs, you may be impacted to these vulnerabilities. The REXML gem 3.4.2 or later include the patches to fix these vulnerabilities.

(CVE-2025-58767)

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://github.com/ruby/rexml/security/advisories/GHSA-c2f4-jgmc-q2r5

Solution

Upgrade to REXML version 3.4.2 or later.

Risk Factor

Medium

CVSS v4.0 Base Score

5.1 (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0001

CVSS v2.0 Base Score

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

STIG Severity

II

References

CVE	CVE-2025-58767
XREF	IAVB:2025-B-0155

Plugin Information

Published: 2025/09/25, Modified: 2025/11/14

Plugin Output

tcp/0

```
Path              : /usr/lib/ruby/gems/3.3.0/gems/rexml-3.3.9
Installed version : 3.3.9
Fixed version     : 3.4.2
```

tcp/0

```
Path              : /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/rexml-3.4.1
Installed version : 3.4.1
Fixed version     : 3.4.2
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=kali
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

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: 2025/11/03

Plugin Output

tcp/0

```
Hostname : kali
  kali (hostname command)
```

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: 2025/09/24

Plugin Output

tcp/0

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

 - 10.0.2.15 (on interface eth0)
 - 127.0.0.1 (on interface lo)
 - 192.168.1.9 (on interface wlan0)
```

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: 2025/09/24

Plugin Output

tcp/0

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

 - fe80::a00:27ff:fe4f:219e (on interface eth0)
 - fd17:625c:f037:2:8dbf:16bb:4267:a86 (on interface eth0)
 - fd17:625c:f037:2:a00:27ff:fe4f:219e (on interface eth0)
 - ::1 (on interface lo)
 - fe80::53e6:89d0:6e7a:4f51 (on interface wlan0)
```

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 addresses exist on the remote host :

  - 08:00:27:4f:21:9e (interface eth0)
  - f0:a7:31:9f:e4:9f (interface wlan0)
```

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

```
wlan0:
  MAC : f0:a7:31:9f:e4:9f
  IPv4:
    - Address : 192.168.1.9
      Netmask : 255.255.255.0
      Broadcast : 192.168.1.255
  IPv6:
    - Address : fe80::53e6:89d0:6e7a:4f51
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
      ScopeID : 0x10
eth0:
  MAC : 08:00:27:4f:21:9e
  IPv4:
    - Address : 10.0.2.15
      Netmask : 255.255.255.0
      Broadcast : 10.0.2.255
  IPv6:
    - Address : fe80::a00:27ff:fe4f:219e
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
    - Address : fd17:625c:f037:2:8dbf:16bb:4267:a86
```

```
        Prefixlen : 64
        Scope : global
        ScopeID : 0x0
    - Address : fd17:625c:f037:2:a00:27ff:fe4f:219e
        Prefixlen : 64
        Scope : global
        ScopeID : 0x0
```

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 :

08:00:27:4F:21:9E : PCS Systemtechnik GmbH
F0:A7:31:9F:E4:9F : TP-Link Systems Inc
```

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: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:4F:21:9E
  - F0:A7:31:9F:E4:9F
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8834/www

```
The remote web server type is :

NessusWWW
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
127.0.0.1 resolves as localhost.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: 3d486b371cacebd11d40ecec34c5bc09
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Mon, 17 Nov 2025 11:42:20 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 1217
  Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self';
 frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src
 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self'
 www.tenable.com; object-src 'none'; base-uri 'self';
  Strict-Transport-Security: max-age=31536000; includeSubDomains
  Expect-CT: max-age=0
```

```
Response Body :

<!doctype html>
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-
src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src
 'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1761337788773" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=0e2ae10949ed6782467b3810ccce69c5" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1761337788773"></script>
        <script src="p [...]
```

147817 - Java Detection and Identification (Linux / Unix)

Synopsis

Java is installed on the remote Linux / Unix host.

Description

One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- This plugin attempts to detect Oracle and non-Oracle JRE instances such as Zulu Java, Amazon Corretto, AdoptOpenJDK, IBM Java, etc

- To discover instances of JRE that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

https://en.wikipedia.org/wiki/Java_(software_platform)

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2025/11/03

Plugin Output

tcp/0

```
Path              : /usr/lib/jvm/java-21-openjdk-amd64/
Version           : 21.0.8
Application       : OpenJDK Java
Binary Location   : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Details           : This Java install appears to be OpenJDK due to the install directory
                    name (high confidence).
Detection Method  : "find" utility
Managed by OS     : True
```

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
udev            921M     0  921M   0% /dev
tmpfs           198M  1.1M  197M   1% /run
/dev/sda1        87G   26G   57G  32% /
tmpfs           987M  4.0K  987M   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           987M  228K  987M   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           198M  124K  198M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 90.3G  0 disk
##sda1   8:1    0 88.3G  0 part /
##sda2   8:2    0    1K  0 part
##sda5   8:5    0    2G  0 part [SWAP]
sr0     11:0    1 1024M  0 rom


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

```
udev on /dev type devtmpfs (rw,nosuid,relatime,size=942712k,nr_inodes=235678,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=600,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=202132k,mode=755,inode64)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2
 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
 (rw,relatime,fd=40,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=4279)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,nosuid,nodev,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec [...]
```

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         : giridhar
Home folder  : /home/giridhar
Start script : /usr/bin/zsh
Groups       : dip
               scanner
               lpadmin
               netdev
               users
               dialout
               wireshark
               video
               vboxsf
               cdrom
               adm
               audio
               sudo
               giridhar
               kaboxer
               bluetooth
               plugdev
               floppy

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

User         : root
Home folder  : /root
Start script : /usr/bin/zsh
```

```
Groups       : root

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

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

User         : sys
Home folder  : /dev
Start script : /usr/sbin/nologin
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

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

User         : man
Home folder  : /var/cache/man
Start script : /usr/sbin/nologin
Groups       : man

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

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

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

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

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

User         : www-data
Home folder  : /var/www
Start script : /usr/sbin/nologin
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /usr/sbin/nologin
Groups       : backup

User         : list
Home folder  : /var/list
Start script : /usr/sbin/nologin
```

```
Groups       : list

 [...]
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

https://www.tenable.com/products/nessus/nessus-professional

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2025/11/03

Plugin Output

tcp/8834/www

```
URL     : https://127.0.0.1:8834/
Version : unknown
```

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 runs on Windows using netstat.exe if the target is localhost (scanner scanning itself) or a Windows host authenticated via SSH with the ability to run netstat.exe.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/10/29

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

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

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) x86_64 GNU/
Linux

Local checks have been enabled for this host.
The remote Debian system is :
kali-rolling

This is a Kali Linux system

OS Security Patch Assessment is available for this host.
Runtime : 2.384479 seconds
```

148373 - OpenJDK Java Detection (Linux / Unix)

Synopsis

A distribution of Java is installed on the remote Linux / Unix host.

Description

One or more instances of OpenJDK Java are installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- Addition information provided in plugin Java Detection and Identification (Unix)

- Additional instances of Java may be discovered by enabling thorough tests

See Also

https://openjdk.java.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/07, Modified: 2025/09/29

Plugin Output

tcp/0

```
Path            : /usr/lib/jvm/java-21-openjdk-amd64/
Version         : 21.0.8
Binary Location : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Managed by OS   : True
```

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: 2025/11/04

Plugin Output

tcp/0

```
Nessus detected 5 installs of OpenSSL:

  Path               : /opt/nessus/bin/openssl
  Version            : 3.0.16
  Associated Package : nessus

  Path               : /usr/lib/x86_64-linux-gnu/ruby/3.3.0/openssl.so
  Version            : 3.5.0
  Associated Package : libruby3.3

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
```

```
  Version            : 3.5.2
  Associated Package : libssl3t64

  Path               : /opt/nessus/lib/nessus/libcrypto.so.3
  Version            : 10.0.16
  Associated Package : nessus

  Path               : /usr/bin/openssl
  Version            : 3.5.2
  Associated Package : openssl 3.5.2-1
  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/lib/x86_64-linux-gnu/libssl.so.3
/opt/nessus/lib/nessus/libssl.so.3
```

232856 - OpenVPN Installed (Linux)

Synopsis

OpenVPN is installed on the remote Linux host.

Description

OpenVPN is installed on the remote Linux host.

Note: Enabling the 'Perform thorough tests' setting will search the file system more broadly.

See Also

https://openvpn.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/19, Modified: 2025/11/03

Plugin Output

tcp/0

```
Path               : /usr/sbin/openvpn
Version            : 2.6.14
Associated Package : openvpn 2.6.14-1
Managed by OS      : True
```

216936 - PHP Scripting Language Installed (Unix)

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly. Thorough test is required to get results on hosts running MacOS.

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/11/05

Plugin Output

tcp/0

```
Path               : /usr/bin/php8.4
Version            : 8.4.11
Associated Package : php8.4-cli: /usr/bin/php8.4
INI file           : /etc/php/8.4/cli/php.ini
INI source         : PHP binary grep
Managed by OS      : True
```

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.
```

130024 - PostgreSQL Client/Server Installed (Linux)

Synopsis

One or more PostgreSQL server or client versions are available on the remote Linux host.

Description

One or more PostgreSQL server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/10/18, Modified: 2025/11/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of PostgreSQL client:

  Path    : /usr/lib/postgresql/17/bin/psql (via package manager)
  Version : 17.5

  Path    : /usr/lib/postgresql/18/bin/psql (via package manager)
  Version : 18.0
```

tcp/0

```
Nessus detected 2 installs of PostgreSQL:

  Path    : /usr/lib/postgresql/17/bin/postgres (via package manager)
  Version : 17.5

  Path    : /usr/lib/postgresql/18/bin/postgres (via package manager)
  Version : 18.0
```

207584 - Ruby Gem Modules Installed (Linux)

Synopsis

Nessus was able to enumerate one or more Ruby Gem modules installed on the remote host.

Description

Nessus was able to enumerate one or more Ruby Gem modules installed on the remote host.
Note that 'Perform thorough tests' may be required for an in-depth search of all Ruby Gem modules.

See Also

http://www.nessus.org/u?26bc7c8b

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/09/23, Modified: 2025/11/12

Plugin Output

tcp/0

```
339 Installed Ruby Gems :

name: Ascii85
version: 2.0.1
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/Ascii85-2.0.1

name: aarch64
version: 2.1.0
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/aarch64-2.1.0

name: abbrev
version: 0.1.2
path: /usr/lib/ruby/gems/3.3.0/gems/abbrev-0.1.2

name: actioncable
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actioncable-7.2.2.2

name: actionmailbox
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionmailbox-7.2.2.2

name: actionmailer
```

```
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionmailer-7.2.2.2

name: actionpack
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionpack-7.2.2.2

name: actiontext
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actiontext-7.2.2.2

name: actionview
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionview-7.2.2.2

name: activejob
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activejob-7.2.2.2

name: activemodel
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activemodel-7.2.2.2

name: activerecord
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activerecord-7.2.2.2

name: activestorage
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activestorage-7.2.2.2

name: activesupport
version: 7.2.2.2
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activesupport-7.2.2.2

name: activesupport
version: 7.2.2.1
path: /usr/share/rubygems-integration/all/specifications/activesupport-7.2.2.1.gemspec

name: addressable
version: 2.8.7
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/addressable-2.8.7

name: afm
version: 1.0.0
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/afm-1.0.0
 [...]
```

202184 - Ruby Programming Language Installed (Linux)

Synopsis

The Ruby programming language is installed on the remote Linux host.

Description

The Ruby programming language is installed on the remote Linux host.

See Also

https://ruby.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/11, Modified: 2025/11/03

Plugin Output

tcp/0

```
Path          : package: ruby3.3  3.3.8-2
Version       : 3.3.8
Managed by OS : True
```

174788 - SQLite Local Detection (Linux / Unix)

Synopsis

The remote Linux host has SQLite Database software installed.

Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, 'Perform thorough tests' setting must be enabled.

See Also

https://www.sqlite.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/26, Modified: 2025/11/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of SQLite:

  Path    : /usr/bin/sqlite3
  Version : 3.46.1

  Path    : /bin/sqlite3
  Version : 3.46.1

Version reported by the package manager.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
This port supports TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: kali

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 52 00

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 17 10:20:54 2025 GMT
Not Valid After: Nov 16 10:20:54 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 5F 38 9B 39 1C 98 4A FE 53 8F 6C E8 45 E9 BC A3 43 B1
```

```
             3C 1E 64 10 44 26 01 B2 B1 6D 2D DA 84 A8 A9 95 4E 3B 2E 06
             FF E3 97 F4 B0 23 D1 BF 5D 86 98 10 6B DD 0C 93 65 1C BD 2C
             A6 9E A7 D8 1F E0 1E 63 39 5E F3 BE 7A 1E F9 34 43 5F F0 D0
             C5 5F 8B 87 EF 45 30 7F 08 8D 66 84 CB F5 6D FC 70 D3 C9 36
             7A BC 71 2E 2F 32 19 38 72 C9 96 77 41 2E A7 A4 62 72 AF 23
             12 E2 6C 09 2D F9 60 1E 58 4A D1 49 3B 21 EC 04 8F 2E C4 62
             66 75 C8 B4 4A 55 3C 06 5A CA 18 F2 E1 79 31 63 A1 56 91 F8
             46 DE 59 F0 AB 14 6B 9A 32 49 22 6D 98 9F BB ED 60 68 AD D4
             48 DA 9B 52 A2 53 F9 96 AF 6B 71 7B 3B B6 69 F6 58 4A 0F 53
             8D BD 0E CD BC B7 19 2A 91 E2 7B FF 21 BE DB 3A 14 46 43 18
             C6 B6 65 86 6F F7 3F 7D EE 9C 83 7B 58 16 83 55 74 DB 71 88
             17 07 86 D7 47 90 18 DB 5E B7 6F 77 A9 B4 C9 D7 A3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8E 88 2E 21 0C 39 4B 6D 19 C4 8C A9 43 7D 63 0C 23 4E 7E
           E1 1E E5 DD A6 FB E8 45 C1 29 5C 72 A8 92 C2 0E 22 61 C6 46
           29 5E 56 15 D3 E9 D7 B4 21 16 38 EA 70 D0 5C 3B 6D 85 74 09
           B5 99 AD C9 7B 3B 43 84 91 5E 0E 8B 8B 0E E5 AB 99 7E 8C B4
           3C 66 EB F2 68 C3 7E 42 89 DA BA 80 98 8A E7 DE EA E5 C3 E0
           CE C2 61 68 09 3A 9E B0 E4 B9 24 16 01 3D ED 78 71 79 67 49
           7E 99 BC DC 9E 3D D8  [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8834/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8834/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

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/8834/www

```
A TLSv1.2 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.2.
```

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 Debian Linux system :

  ii   7zip  25.01+dfsg-2  amd64  7-Zip file archiver with a high compression ratio
  ii   accountsservice  23.13.9-7  amd64  query and manipulate user account information
  ii   acl  2.3.2-2+b1  amd64  access control list - utilities
  ii   adduser  3.152  all  add and remove users and groups
  ii   adwaita-icon-theme  48.1-1  all  default icon theme of GNOME
  ii   aircrack-ng  1:1.7+git20230807.4bf83f1a-2+b1  amd64  wireless WEP/WPA cracking utilities
  ii   alsa-topology-conf  1.2.5.1-3  all  ALSA topology configuration files
  ii   alsa-ucm-conf  1.2.14-1  all  ALSA Use Case Manager configuration files
  ii   amass  4.2.0-0kali1  amd64  In-depth DNS Enumeration and Network Mapping
  ii   amass-common  4.2.0-0kali1  all  In-depth DNS Enumeration and Network Mapping
  ii   amd64-microcode  3.20250311.1  amd64  Platform firmware and microcode for AMD CPUs and SoCs
  ii   apache2  2.4.65-3+b1  amd64  Apache HTTP Server
  ii   apache2-bin  2.4.65-3+b1  amd64  Apache HTTP Server (modules and other binary files)
  ii   apache2-data  2.4.65-3  all  Apache HTTP Server (common files)
  ii   apache2-utils  2.4.65-3+b1  amd64  Apache HTTP Server (utility programs for web servers)
  ii   apparmor  4.1.0-1  amd64  user-space parser utility for AppArmor
  ii   apt  3.1.4+kali1  amd64  commandline package manager
  ii   apt-file  3.3  all  search for files within Debian packages (command-line interface)
  ii   apt-utils  3.1.4+kali1  amd64  package management related utility programs
  ii   arj  3.10.22-28  amd64  archiver for .arj files
```

```
ii   arp-scan  1.10.0-2+b1  amd64  arp scanning and fingerprinting tool
ii   arping  2.26-1  amd64  sends IP and/or ARP pings (to the MAC address)
ii   aspell  0.60.8.1-4  amd64  GNU Aspell spell-checker
ii   aspell-en  2020.12.07-0-1  all  English dictionary for GNU Aspell
ii   aspnetcore-runtime-6.0  6.0.8-1  amd64
ii   aspnetcore-targeting-pack-6.0  6.0.9-1  amd64
ii   at-spi2-common  2.57.1-1  all  [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :

Strict-Transport-Security: max-age=31536000; includeSubDomains
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

163326 - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

https://www.tenable.com/products/nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/11/03

Plugin Output

tcp/0

```
Path    : /opt/nessus
Version : 10.10.1
Build   : 20010
```

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: 2025/11/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.8.1
  Version            : 5.8.1
  Associated Package : liblzma-dev 5.8.1-1
  Confidence         : High
```

```
   Managed by OS      : True
   Version Source     : Package

   Path               : /usr/bin/xz
   Version            : 5.8.1
   Associated Package : xz-utils 5.8.1-1
   Confidence         : High
   Managed by OS      : True
   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  0.0  0.4  24156  9060 ?        Ss   16:05   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    16:05   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    16:05   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-sync_wq]
root           7  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-netns]
root          13  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0      0     0 ?        I    16:05   0:00 [rcu_tasks_kthread]
root          15  0.0  0.0      0     0 ?        I    16:05   0:00 [rcu_tasks_rude_kthread]
root          16  0.0  0.0      0     0 ?        I    16:05   0:00 [rcu_tasks_trace_kthread]
root          17  0.1  0.0      0     0 ?        S    16:05   0:07 [ksoftirqd/0]
root          18  0.0  0.0      0     0 ?        I    16:05   0:03 [rcu_preempt]
root          19  0.0  0.0      0     0 ?        S    16:05   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          20  0.0  0.0      0     0 ?        S    16:05   0:00 [rcu_exp_gp_kthread_worker]
root          21  0.0  0.0      0     0 ?        S    16:05   0:00 [migration/0]
root          22  0.0  0.0      0     0 ?        S    16:05   0:00 [idle_inject/0]
root          23  0.0  0.0      0     0 ?        S    16:05   0:00 [cpuhp/0]
root          25  0.0  0.0      0     0 ?        S    16:05   0:00 [kdevtmpfs]
root          26  0.0  0.0      0     0 ?        I<   16:05   0:00 [kworker/R-inet_frag_wq]
root          27  0.0  0.0      0     0 ?        S    16:05   0:00 [kauditd]
root          28  0.0  0.0      0     0 ?        S    16:05  [...]
```

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: 2025/11/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 9.1

  Path    : /usr/bin/vim.basic
  Version : 9.1
```