Localhost Vulnerability Scan

Report generated by Tenable Nessus™ Tue, 17 Feb 2026 00:14:56 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

127.0.0.1

1	3	7	1	75
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Feb 17 00:00:03 2026
End time:	Tue Feb 17 00:14:55 2026

Host Information

IP:	127.0.0.1
MAC Address:	08:00:27:1F:B7:23
OS:	Linux Kernel 6.18.9+kali-amd64

Vulnerabilities

278743 - Tenable Nessus 10.8.0 <= 10.8.6 / 10.9.0 < 10.9.6 / 10.10.0 <= 10.10.1 / 10.11.0 < 10.11.1 Multiple Vulnerabilities (TNS-2025-24)

Synopsis

An instance of Nessus installed on the remote system is affected by multiple vulnerabilities.

Description

According to its self-reported version, the Tenable Nessus application running on the remote host is 10.8.0 prior or equal to 10.8.6, 10.9.0 prior to 10.9.6, 10.10.0 prior or equal to 10.10.1 and 10.11.0 prior to 10.11.1. It is, therefore, affected by multiple vulnerabilities as referenced in the TNS-2025-24 advisory.

- xsltGetInheritedNsList in libxslt before 1.1.43 has a use-after-free issue related to exclusion of result prefixes. (CVE-2024-55549)

- A use-after-free vulnerability was found in libxml2. This issue occurs when parsing XPath elements under certain circumstances when the XML schematron has the <sch:name path=.../> schema elements. This flaw allows a malicious actor to craft a malicious XML document used as input for libxml, resulting in the program's crash using libxml or other possible undefined behaviors. (CVE-2025-49794)

- A vulnerability was found in libxml2. Processing certain sch:name elements from the input XML file can trigger a memory corruption issue. This flaw allows an attacker to craft a malicious XML input file that can lead libxml to crash, resulting in a denial of service or other possible undefined behavior due to sensitive data being corrupted in memory. (CVE-2025-49796)

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://docs.tenable.com/release-notes/Content/nessus/2025.htm#10.9.6

https://docs.tenable.com/release-notes/Content/nessus/2025.htm#10.11.1

https://www.tenable.com/security/TNS-2025-24

Solution

Upgrade to Tenable Nessus 10.9.6, 10.11.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

7.9

EPSS Score

0.0069

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2024-8176
CVE	CVE-2024-55549
CVE	CVE-2025-6021
CVE	CVE-2025-6170
CVE	CVE-2025-7425
CVE	CVE-2025-10911
CVE	CVE-2025-11731
CVE	CVE-2025-49794
CVE	CVE-2025-49796
CVE	CVE-2025-59375
XREF	IAVA:2026-A-0153

Plugin Information

Published: 2025/12/16, Modified: 2026/02/13

Plugin Output

tcp/0

```

  Path              : /opt/nessus
  Installed version : 10.10.1
  Fixed version     : 10.11.1
```

236779 - Ruby RACK < 2.2.14 / 3.0.16 / 3.1.14 DoS vulnerability

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 2.2.14 / 3.0.16 / 3.1.14 . It is, therefore, affected by a DoS vulnerability where an attacker can trigger denial of service by sending specifically crafted HTTP requests, which can cause memory exhaustion or pin CPU resources, stalling or crashing the Rack server. This results in full service disruption until the affected worker is restarted.

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-gjh7-p2fx-99vx

Solution

Upgrade to RACK version 2.2.14 / 3.0.16 / 3.1.14 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

3.6

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
XREF	IAVA:2025-B-0073-S

Plugin Information

Published: 2025/05/15, Modified: 2025/10/17

Plugin Output

tcp/0

```
Path              : /usr/share/beef-xss/vendor/bundle/ruby/3.3.0/gems/rack-2.2.13
Installed version : 2.2.13
Fixed version     : 2.2.14
```

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

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

3.6

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/beef-xss/vendor/bundle/ruby/3.3.0/gems/rack-2.2.13
  Installed version : 2.2.13
  Fixed version     : 2.2.20
```

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

3.6

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-S

Plugin Information

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

Plugin Output

tcp/0

```
  Path              : /usr/share/beef-xss/vendor/bundle/ruby/3.3.0/gems/rack-2.2.13
  Installed version : 2.2.13
  Fixed version     : 2.2.19
```

282519 - Apache Log4j 2.0-beta9 < 2.25.3 MitM

Synopsis

A logging library installed on the remote host is affected by a man in the middle vulnerability.

Description

The version of Apache Log4j on the remote host is 2.0-beta9 through 2.25.2. The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25.2 does not perform TLS hostname verification of the peer certificate, even when the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName configuration attribute or the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property is set to true. This issue may allow a man-in-the-middle attacker to intercept or redirect log traffic under the following conditions:

- The attacker is able to intercept or redirect network traffic between the client and the log receiver.

- The attacker can present a server certificate issued by a certification authority trusted by the Socket Appender's configured trust store (or by the default Java trust store if no custom trust store is configured).

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://lists.apache.org/thread/xr33kyxq3sl67lwb61ggvm1fzc8k7dvx

Solution

Upgrade to Apache Log4j version 2.25.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.0

EPSS Score

0.0003

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

STIG Severity

I

References

CVE	CVE-2025-68161
XREF	IAVA:2026-A-0001

Plugin Information

Published: 2026/01/09, Modified: 2026/01/09

Plugin Output

tcp/0

```
  Path              : /usr/share/zaproxy/lib/log4j-core-2.25.2.jar
  Installed version : 2.25.2
  Fixed version     : 2.25.3
```

tcp/0

```
  Path              : /usr/share/zaproxy/lib/log4j-jul-2.25.2.jar
  Installed version : 2.25.2
  Fixed version     : 2.25.3
```

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: 2025/11/18

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
```

298656 - Vim < 9.1.2132 Buffer Overflow (GHSA-5w93-4g67-mm43)

Synopsis

The remote host is missing a security update.

Description

The version of Vim installed on the remote host is prior to 9.1.2132. It is, therefore, affected by a vulnerability as referenced in the GHSA-5w93-4g67-mm43 advisory.

- Vim is an open source, command line text editor. Prior to version 9.1.2132, a heap buffer overflow vulnerability exists in Vim's tag file resolution logic when processing the 'helpfile' option. The vulnerability is located in the get_tagfname() function in src/tag.c. When processing help file tags, Vim copies the user-controlled 'helpfile' option value into a fixed-size heap buffer of MAXPATHL + 1 bytes (typically 4097 bytes) using an unsafe STRCPY() operation without any bounds checking. This issue has been patched in version 9.1.2132. (CVE-2026-25749)

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

See Also

http://www.nessus.org/u?c87397b9

Solution

Upgrade to Vim version 9.1.2132 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2026-25749
XREF	IAVA:2026-A-0138

Plugin Information

Published: 2026/02/11, Modified: 2026/02/13

Plugin Output

tcp/0

```
  Path              : /usr/bin/vim.basic
  Installed version : 9.1
  Fixed version     : 9.1.2132
```

tcp/0

```
  Path              : /usr/bin/vim.tiny
  Installed version : 9.1
  Fixed version     : 9.1.2132
```

298226 - Tenable Nessus < 10.10.2 / 10.11.0 < 10.11.2 Multiple Vulnerabilities (TNS-2026-04)

Synopsis

An instance of Nessus installed on the remote system is affected by multiple vulnerabilities.

Description

According to its self-reported version, the Tenable Nessus application running on the remote host prior to 10.10.2, 10.11.0 prior to 10.11.2. It is, therefore, affected by multiple vulnerabilities as referenced in the TNS-2026-04 advisory.

- In libexpat before 2.7.4, XML_ExternalEntityParserCreate does not copy unknown encoding handler user data.

(CVE-2026-24515)

- In libexpat before 2.7.4, the doContent function does not properly determine the buffer size bufSize because there is no integer overflow check for tag buffer reallocation. (CVE-2026-25210)

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://docs.tenable.com/release-notes/Content/nessus/nessus.htm

https://www.tenable.com/security/TNS-2026-04

Solution

Upgrade to Tenable Nessus 10.10.2, 10.11.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.0

EPSS Score

0.0001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2026-24515
CVE	CVE-2026-25210

Plugin Information

Published: 2026/02/06, Modified: 2026/02/09

Plugin Output

tcp/0

```
Path              : /opt/nessus
Installed version : 10.10.1
Fixed version     : 10.10.2
```

141394 - Apache HTTP Server Installed (Linux)

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2026/02/03

Plugin Output

tcp/0

```
Path               : /usr/sbin/apache2
Version            : 2.4.66
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS      : True
Running            : no

Configs found :
  - /etc/apache2/apache2.conf

Loaded modules :
  - libphp8.4
  - mod_access_compat
  - mod_alias
  - mod_auth_basic
  - mod_authn_core
  - mod_authn_file
  - mod_authz_core
  - mod_authz_host
```

```
      - mod_authz_user
      - mod_autoindex
      - mod_deflate
      - mod_dir
      - mod_env
      - mod_filter
      - mod_mime
      - mod_mpm_prefork
      - mod_negotiation
      - mod_reqtimeout
      - mod_setenvif
      - mod_status
```

142640 - Apache HTTP Server Site Enumeration

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/09, Modified: 2026/01/05

Plugin Output

tcp/0

```
Sites and configs present in /usr/sbin/apache2 Apache installation:
  - following sites are present in /etc/apache2/apache2.conf Apache config file:
    +  () - *:80
```

156000 - Apache Log4j Installed (Linux / Unix)

Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

Note, this plugin runs certain commands differently if the scan is configured to use the 'Attempt Least Privilege' option. If enabled, scan times are expected to increase, especially on hosts with many files.

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

See Also

https://logging.apache.org/log4j/2.x/

Solution

n/a

Risk Factor

None

References

XREF	IAVA:0001-A-0650
XREF	IAVT:0001-T-0941

Plugin Information

Published: 2021/12/10, Modified: 2026/02/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of Apache Log4j:

  Path                          : /usr/share/zaproxy/lib/log4j-jul-2.25.2.jar
  Version                       : 2.25.2
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
```

```
    JndiLookup.class association   : Not Found
    Method                         : MANIFEST.MF dependency

    Path                           : /usr/share/zaproxy/lib/log4j-core-2.25.2.jar
    Version                        : 2.25.2
    JMSAppender.class association  : Found
    JdbcAppender.class association : Found
    JndiLookup.class association   : Found
    Method                         : log4j-core file search
```

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: 2026/01/05

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.66 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:log4j:2.25.2 -> Apache Software Foundation log4j
  cpe:/a:exiv2:exiv2:0.28.7 -> Exiv2
  cpe:/a:exiv2:libexiv2:0.28.7
  cpe:/a:gnupg:libgcrypt:1.11.3 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:8.18.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.18.0 -> Haxx libcurl
  cpe:/a:imagemagick:imagemagick:7.1.2.1 -> ImageMagick
  cpe:/a:jmcnamara:spreadsheet%3a%3aparseexcel:0.66 -> John McNamara Spreadsheet::ParseExcel
  cpe:/a:nginx:nginx:1.28.1 -> Nginx
  cpe:/a:nginx:nginx:1.28.1-3 -> Nginx
  cpe:/a:nodejs:node.js:22.22.0 -> Nodejs Node.js
```

```
    cpe:/a:numpy:numpy:2.3.5 -> NumPy
    cpe:/a:openssl:openssl:10.0.16 -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:3.0.16 -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:3.5.0 -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:3.5.4 -> OpenSSL Project OpenSSL
    cpe:/a:openvpn:openvpn:2.7.0 -> OpenVPN
    cpe:/a:oracle:openjdk:21.0.10 -> Oracle OpenJDK -
    cpe:/a:php:php:8.4.16 -> PHP PHP
    cpe:/a:postgresql:postgresql:17.6 -> PostgreSQL
    cpe:/a:postgresql:postgresql:18.1 -> PostgreSQL
    cpe:/a:ruby-lang:ruby:3.3.8 -> Ruby-lang Ruby
    cpe:/a:sqlite:sqlite:3.46.1 -> SQLite
    cpe:/a:tenable:nessus -> Tenable Nessus
    cpe:/a:tenable:nessus:10.10.1 -> Tenable Nessus
    cpe:/a:tornadoweb:tornado:6.5.4 -> Tornado Web Server Tornado
    cpe:/a:tukaani:xz:5.8.2 -> Tukaani XZ
    cpe:/a:vim:vim:9.1 -> Vim
    x-cpe:/a:java:jre:21.0.10
    x-cpe:/a:libndp:libndp:1.9
```

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: 2026/02/03

Plugin Output

tcp/0

```
  Path               : /usr/bin/curl
  Version            : 8.18.0
  Associated Package : curl 8.18.0-2
  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: 2026/02/03

Plugin Output

tcp/0

```

  Hostname : kali
    kali (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 : 99
```

159273 - Dockerfile Detection for Linux/UNIX

Synopsis

Detected Dockerfiles on the host.

Description

The host contains Dockerfiles, text files containing instructions to build Docker images.

See Also

https://docs.docker.com/engine/reference/builder/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/03/29, Modified: 2026/02/03

Plugin Output

tcp/0

```
Dockerfiles found: 14
  - /home/kali/CeWL/Dockerfile
  - /home/kali/Downloads/CyberChef/Dockerfile
  - /home/kali/Photon/Dockerfile
  - /home/kali/sherlock/Dockerfile
  - /home/kali/theHarvester/Dockerfile
  - /usr/lib/python3/dist-packages/dirsearch/Dockerfile
  - /usr/share/metasploit-framework/data/exploits/CVE-2025-8518/Dockerfile
  - /usr/share/metasploit-framework/data/exploits/react2shell_unauth_rce_cve_2025_55182/Dockerfile
  - /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile
  - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ssh-7.3.0/Dockerfile
  - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/pg-1.6.3-x86_64-linux/misc/glibc/
Dockerfile
  - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/pg-1.6.3-x86_64-linux/misc/
yugabyte/Dockerfile
  - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/puma-7.2.0/tools/Dockerfile
  - /usr/share/nmap/scripts/vulscan/utilities/docker/Dockerfile
```

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 :

 - 192.168.1.15 (on interface eth0)
 - 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: 2025/09/24

Plugin Output

tcp/0

```

The following IPv6 interfaces are set on the remote host :

 - fe80::eb5c:9e04:124c:c95b (on interface eth0)
 - ::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 :

  - 08:00:27:1f:b7:23 (interface eth0)
```

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
eth0:
  MAC : 08:00:27:1f:b7:23
  IPv4:
    - Address : 192.168.1.15
        Netmask : 255.255.255.0
        Broadcast : 192.168.1.255
  IPv6:
    - Address : fe80::eb5c:9e04:124c:c95b
        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:
  eth0:
    ipv4_gateways:
      192.168.1.1:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  eth0:
    ipv4_subnets:
     - 192.168.1.0/24
    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: 2026/02/03

Plugin Output

tcp/0

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

/usr/local/sbin
/usr/local/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 :

08:00:27:1F:B7:23 : 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: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:1F:B7:23
```

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: 2026/02/03

Plugin Output

tcp/0

```
  Path               : /usr/bin/exiv2
  Version            : 0.28.7
  Associated Package : exiv2 0.28.7
  Managed by OS      : True
```

168982 - Filepaths contain Dangerous characters (Linux)

Synopsis

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.

Description

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.

This product has chosen in certain plugins to avoid digging within those files and directories for security reasons.

These should be renamed to avoid security compromise.

Solution

Rename these files or folders to not include dangerous characters.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2024/07/24

Plugin Output

tcp/22

```
The following files and directories contain potentially dangerous characters such as brackets,
 ampersand, or semicolon.
This scanner avoided access to these files when possible for safety:

/usr/share/node_modules/@babel/core/lib/config
/usr/share/node_modules/@babel/eslint-shared-fixtures/config
/usr/share/node_modules/@npmcli/config
/usr/share/nodejs/@babel/core/lib/config
/usr/share/nodejs/@babel/eslint-shared-fixtures/config
/usr/share/nodejs/@npmcli/config
```

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: b77c9e9e0587e0a5c3e636da1ecf0107
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Tue, 17 Feb 2026 05:00:30 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=700436ae07ed6e12f2bad5aa014d5023" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1761337788773"></script>
        <script src="p [...]
```

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: 2026/02/03

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address        : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address        : ::1
      Assign Method : static
+ eth0
  + IPv4
    - Address        : 192.168.1.15
      Assign Method : dynamic
  + IPv6
    - Address        : fe80::eb5c:9e04:124c:c95b
      Assign Method : static
```

278763 - ImageMagick Installed (Linux)

Synopsis

ImageMagick is installed on the remote Linux host.

Description

ImageMagick Tool is installed on the remote Linux host.

Additional information:

- 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://ImageMagick.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/16, Modified: 2026/02/03

Plugin Output

tcp/0

```
  Path    : unknown (Package: imagemagick  8:7.1.2.13)
  Version : 7.1.2-1
```

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: 2026/02/09

Plugin Output

tcp/0

```
  Path             : /usr/lib/jvm/java-21-openjdk-amd64/
  Version          : 21.0.10
  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
```

189990 - Jmcnamara Spreadsheet-ParseExcel Installed (Unix)

Synopsis

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

Description

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

See Also

https://github.com/jmcnamara/spreadsheet-parseexcel

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/05, Modified: 2026/02/03

Plugin Output

tcp/0

```
  Path               : /usr/share/perl5/Spreadsheet/ParseExcel.pm
  Version            : 0.66
  Associated Package : libspreadsheet-parseexcel-perl: /usr/share/perl5/Spreadsheet/ParseExcel.pm
  Managed by OS      : True
```

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: 2026/02/03

Plugin Output

tcp/0

```

Nessus detected 4 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.3

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.6.0
  Version : 1.11.3

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.3

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.6.0
  Version : 1.11.3
```

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp 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.200214' 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://github.com/jpirko/libndp

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2026/02/03

Plugin Output

tcp/0

```
  Path           : libndp0 1.9-1 (via package manager)
  Version        : 1.9
  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            3.2G     0  3.2G   0% /dev
tmpfs           676M  988K  675M   1% /run
/dev/sda1        79G   36G   39G  48% /
tmpfs           3.3G  4.0K  3.3G   1% /dev/shm
none            1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           3.3G  8.0K  3.3G   1% /tmp
none            1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           676M  120K  676M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 80.1G  0 disk
##sda1   8:1    0 80.1G  0 part /
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=3354232k,nr_inodes=838558,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=692016k,mode=755,inode64)
```

```
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro) [root]
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,memory_hugetlb_accounting)
none 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=41,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=5272)
none on /run/credentials/systemd-journald.service type tmpfs
 (ro,nosuid,nodev,noexec,relatime,nosymfollow,size=1024k,nr_inodes=1024,mode=700,inode64,noswap)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,nosuid,nodev,relatime,pagesize=2M)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
debugfs on /sy [...]
```

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: EST -0500
Via timedatectl: Time zone: America/New_York (EST, -0500)
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

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

User         [...]
```

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: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.10.1
Nessus build : 20010
Plugin feed version : 202602152114
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Localhost Vulnerability Scan
Scan policy used : Basic Network Scan
Scanner IP : 127.0.0.1
Ping RTT : Unavailable
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 : yes
Credentialed checks : yes (on the localhost)
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 : 2026/2/17 0:00 EST (UTC -05:00)
Scan duration : 889 sec
Scan for malware : no
```

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
```

178771 - Node.js Installed (Linux / UNIX)

Synopsis

Node.js is installed on the remote Linux / UNIX host.

Description

Node.js is installed on the remote Linux / UNIX host.

See Also

https://nodejs.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/07/25, Modified: 2026/02/03

Plugin Output

tcp/0

```
  Path            : /usr/bin/node
  Version         : 22.22.0
  Managed         : 1
  Package         : nodejs
  Package release : 1+b1
  Package version : 22.22.0+dfsg+~cs22.19.6

  aliases :
    - /bin/node
    - /bin/nodejs
    - /usr/bin/nodejs
```

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 : Linux Kernel 6.18.9+kali-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux kali 6.18.9+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.18.9-1kali1
 (2026-02-10) x86_64 GNU/Linux


Following fingerprints could not be used to determine OS :
 HTTP:!:Server: NessusWWW

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:kalis/O:Nessus Users Uniteds/OU:Nessus Server
21031dea6ae30b6cf3212356b77fb5634191ea11
```

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: 2025/06/03

Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 6.18.9+kali-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.18.9+kali-amd64
```

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 6.18.9+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.18.9-1kali1 (2026-02-10) 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 : 1.906998 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.

Protocol : LOCAL
```

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         : 21.0.10
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: 2026/02/03

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            : 3.5.4
  Associated Package : libssl3t64

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

  Path               : /usr/bin/openssl
  Version            : 3.5.4
  Associated Package : openssl 3.5.4-1
  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: 2026/02/03

Plugin Output

tcp/0

```
Path               : /usr/sbin/openvpn
Version            : 2.7.0
Associated Package : openvpn 2.7.0
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: 2026/02/03

Plugin Output

tcp/0

```
  Path               : /usr/bin/php8.4
  Version            : 8.4.16
  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.
```

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: 2026/02/10

Plugin Output

tcp/0

```

. You need to take the following 5 actions :


[ Apache Log4j 2.0-beta9 < 2.25.3 MitM (282519) ]

+ Action to take : Upgrade to Apache Log4j version 2.25.3 or later.


[ Ruby RACK < 2.2.20 / 3.x < 3.1.18 / 3.2 < 3.2.3 Multiple Vulnerabilities (270698) ]

+ Action to take : Upgrade to RACK version 2.2.20 / 3.1.18 / 3.2.3 or later.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).



[ Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability (265895) ]

+ Action to take : Upgrade to REXML version 3.4.2 or later.


[ Tenable Nessus < 10.10.2 / 10.11.0 < 10.11.2 Multiple Vulnerabilities (TNS-2026-04) (298226) ]

+ Action to take : Upgrade to Tenable Nessus 10.10.2, 10.11.2 or later.
```

```
+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).


[ Vim < 9.1.2132 Buffer Overflow (GHSA-5w93-4g67-mm43) (298656) ]

+ Action to take : Upgrade to Vim version 9.1.2132 or later.
```

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: 2026/02/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of PostgreSQL client:

  Path    : /usr/lib/postgresql/17/bin/psql (via package manager)
  Version : 17.6

  Path    : /usr/lib/postgresql/18/bin/psql (via package manager)
  Version : 18.1
```

tcp/0

```
Nessus detected 2 installs of PostgreSQL:

  Path    : /usr/lib/postgresql/17/bin/postgres (via package manager)
  Version : 17.6

  Path    : /usr/lib/postgresql/18/bin/postgres (via package manager)
  Version : 18.1
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.

However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2025/12/08

Plugin Output

tcp/8834/www

```
The target TLS server offers no post-quantum ciphers.
```

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: 2026/02/03

Plugin Output

tcp/0

```

401 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: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actioncable-7.2.3

name: actionmailbox
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionmailbox-7.2.3

name: actionmailer
```

```
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionmailer-7.2.3

name: actionpack
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionpack-7.2.3

name: actiontext
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actiontext-7.2.3

name: actionview
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/actionview-7.2.3

name: activejob
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activejob-7.2.3

name: activemodel
version: 7.2.2.1
path: /usr/share/beef-xss/vendor/bundle/ruby/3.3.0/gems/activemodel-7.2.2.1

name: activemodel
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activemodel-7.2.3

name: activerecord
version: 7.2.2.1
path: /usr/share/beef-xss/vendor/bundle/ruby/3.3.0/gems/activerecord-7.2.2.1

name: activerecord
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activerecord-7.2.3

name: activestorage
version: 7.2.3
path: /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/activestorage-7.2.3

name: activesupport
version: 7.2.2.2
path: /usr/share/rubygems-integration/all/specifications/activesupport-7.2.2.2.gemspec

name: activesupport
version: 7.2.2.1
path: /usr/share/beef-xss/vendor/bundle/ruby/3.3.0/gems/activesupport-7.2.2.1

name: activesupport
version: 7.2.3
path: /usr/sha [...]
```

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: 2026/02/03

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: 2026/02/03

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: 6E FC

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 06 06:50:58 2025 GMT
Not Valid After: Nov 05 06:50:58 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C3 23 FF 0C A1 EE 35 7F 55 3F 59 AB AB 94 FC 2A 43 C1 B4
```

```
            2C F9 87 A3 57 64 3F 6E 5D 32 BD 8D C1 2E 63 67 4A 65 8B C5
            21 15 EA 7D 00 E2 75 33 DA B6 A0 F1 25 39 C8 B6 A7 ED 68 3E
            D8 7B 6F 31 F7 43 88 F4 86 54 5F DA F0 20 1D CB 2F CF 4B 18
            22 4A D9 C3 E1 FC 67 B7 C8 E0 D1 CA 17 06 D5 8F EC F3 82 91
            93 1E 40 EF DA B6 10 3F 09 B7 8B B2 E2 52 2A 6B AB 7D 73 34
            70 D6 9A D4 6E 07 70 4A 08 7E 84 83 59 87 9F 77 8D 32 7F 6A
            37 4C 71 7E 49 70 3B 9F 12 A2 6E 97 F3 0A 0D B9 F9 33 DB 83
            0F 84 EA B6 89 87 AE C4 43 F8 2F 94 0B 5B 2E F2 F4 48 2A EE
            C1 14 D0 D9 AA A8 76 B2 C8 6F A0 6D 6F D5 DF 92 49 23 37 EE
            A1 0B 4D 67 E1 C1 B6 15 81 35 4B 9D 10 28 95 93 62 62 3E 2B
            42 6E 74 69 4C D8 7C 62 61 ED 05 76 35 FF 24 8D BD 0B 01 EA
            48 45 4F 8E 63 D3 B7 C9 36 02 E6 CC 1A 3D C6 73 AF
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 10 5C CB 49 5B B1 D1 59 7E 86 DC 24 A0 79 47 CC 90 51 9E
           01 BE 42 6E A8 DE 0B 1C 8B D9 58 3A 30 B5 93 30 6C 87 76 75
           30 01 EB 79 8A D9 0F 48 EA 5E 36 A0 BE A7 03 72 AC 8F DF A2
           D7 78 4F 1C 37 7B 18 A5 7A AE 44 C3 24 1C A1 54 DD E0 1F 24
           81 AD A8 A9 CE C5 3A C7 17 39 54 C6 A9 17 09 06 94 66 CF B9
           DF FC FC BE 8F D2 07 E5 A9 FF 7C 8A F5 51 73 64 0F E9 88 41
           A8 DC 84 05 35 13 30  [...]
```

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_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 SHA384


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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         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       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         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: 2026/02/02

Plugin Output

tcp/8834/www

```
A TLSv1.3 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.3.
```

298387 - Shor's Harvest Now Decrypt Later

Synopsis

Reports remote services potentially vulnerable to Shor's Algorithm.

Description

This plugin reports network services that may be vulnerable now to a future attack by adversaries using a cryptographically relevant quantum computer (CRQC). Shor's is a theoretical algorithm that leverages the unique ability of quantum computation to do massively parallel calculations developed by Peter Shor in 1994.

This algorithm easily computes two classically difficult mathematical problems used in modern cryptography; discrete logarithms, and factoring numbers formed by multiplying large primes. Shor's reduces both of these problems from taking exponential time in chosen cases to being solvable in polynomial time.

Asymmetric encryption algorithms such as RSA, Diffie-Hellman and Elliptic Curve Diffie-Hellman are impacted by Shor's Algorithm. The most common uses of these algorithms are in symmetric key establishment and authentication. These uses render Shor's Algorithm particularly dangerous because it may give an adversary the ability to harvest network communications now, and in the future, when a CRQC becomes available, extract the symmetric key and decrypt the communication.

See Also

http://www.nessus.org/u?54fba2c1

Solution

Replace affected ciphers with algorithms chosen to resist CRQC attack.

Risk Factor

None

Plugin Information

Published: 2026/02/09, Modified: 2026/02/09

Plugin Output

tcp/0

```
The TLS service on port 8834 offers these ciphers vulnerable to Shor's:
TLS_AES_256_GCM_SHA384 with curves:
ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, secp384r1, secp521r1, x448, secp256r1 or
 x25519
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 with curves:
x25519, secp256r1, x448, secp521r1 or secp384r1
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 with curves:
x25519, secp256r1, x448, secp521r1 or secp384r1
```

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-5  amd64  7-Zip file archiver with a high compression ratio
  ii  aapt  1:14~beta1-5  amd64  Android Asset Packaging Tool
  ii  accountsservice  23.13.9-8+b1  amd64  query and manipulate user account information
  ii  acl  2.3.2-2+b2  amd64  access control list - utilities
  ii  adduser  3.154  all  add and remove users and groups
  ii  adwaita-icon-theme  49.0-1  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  1.2.15.3-1  all  ALSA Use Case Manager configuration files
  ii  amass  5.0.1-0kali4  amd64  In-depth DNS Enumeration and Network Mapping
  ii  amd64-microcode  3.20251202.1  amd64  Platform firmware and microcode for AMD CPUs and SoCs
  ii  android-framework-res  1:14~beta1-5  all  Android platform framework resources
  ii  android-libaapt  1:14~beta1-5  amd64  Android Asset Packaging Tool - Shared library
  ii  android-libandroidfw  1:14~beta1-5  amd64  Android utility library
  ii  android-libbacktrace  1:34.0.5-12+b1  amd64  Android backtrace library
  ii  android-libbase  1:34.0.5-12+b1  amd64  Android base library
  ii  android-libcutils  1:34.0.5-12+b1  amd64  Android utils library for C
  ii  android-liblog  1:34.0.5-12+b1  amd64  Android NDK logger interfaces
  ii  android-libutils  1:34.0.5-12+b1  amd64  Android Utility Function Library
  ii  android-libziparchive  1:34.0.5-12+b1  amd64  Library for ZIP archives
```

```
    ii   apache2  2.4.66-6  amd64  Apache HTTP Server
    ii   apache2-bin  2.4.66-6  amd64  Apache HTTP Server (modules and other binary files)
    ii   apache2-data  2.4.66-6  all  Apache HTTP Server (common files)
    ii   apache2-utils  2.4.66-6  amd64  Apache HTTP Server (utility programs for web servers)
    ii   apparmor  4.1.3-1  amd64  user-space parser utility for AppArmor
    ii   apt  3.1.14+kali1  [...]
```

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
```

277654 - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/08, Modified: 2026/01/20

Plugin Output

tcp/8834/www

```

These are the TLS supported groups offered by the remote server :


TLS supported groups :

Name                    Code
--------------------------
secp521r1               0x0019
ffdhe3072               0x0101
ffdhe4096               0x0102
secp384r1               0x0018
ffdhe8192               0x0104
x448                    0x001e
x25519                  0x001d
secp256r1               0x0017
ffdhe6144               0x0103
ffdhe2048               0x0100
```

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.
```

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2025/08/28

Plugin Output

tcp/0

```
Nessus was able to execute commands locally with sufficient privileges
for all planned checks.
```

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/0

```
Nessus was able to execute commands on localhost.
```

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: 2026/02/03

Plugin Output

tcp/0

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

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

```
The host has not yet been rebooted.
```

237200 - Tornado Detection

Synopsis

A Tornado Python library is installed on the remote host.

Description

A Tornado Python library is installed on the remote host.

Note that Nessus has relied upon on the application's self-reported version number.

See Also

https://python.Tornado.com/v0.1/docs/get_started/quickstart/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/23, Modified: 2026/02/05

Plugin Output

tcp/0

```
  Path               : /usr/lib/python3/dist-packages/tornado-6.5.4.egg-info
  Version            : 6.5.4
  Associated Package : python3-tornado
  Managed by OS      : True
```

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: 2026/02/03

Plugin Output

tcp/0

```

Nessus detected 2 installs of XZ Utils:

  Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.8.2
  Version            : 5.8.2
  Associated Package : liblzma-dev 5.8.2-2
  Confidence         : High
  Managed by OS      : True
  Version Source     : Package

  Path               : /usr/bin/xz
  Version            : 5.8.2
  Associated Package : xz-utils 5.8.2-2
  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  0.2  24852 15628 ?        Ss   Feb16   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    Feb16   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    Feb16   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-kvfree_rcu_reclaim]
root           7  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-netns]
root          13  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0      0     0 ?        S    Feb16   0:03 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    Feb16   0:07 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    Feb16   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          17  0.0  0.0      0     0 ?        S    Feb16   0:00 [rcu_exp_gp_kthread_worker]
root          18  0.0  0.0      0     0 ?        S    Feb16   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    Feb16   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    Feb16   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    Feb16   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    Feb16   0:00 [idle_inject/1]
root          23  0.0  0.0      0     0 ?        S    Feb16   0:01 [migration/1]
root          24  0.0  0.0      0     0 ?        S    Feb16   0:01 [ksoftirqd/1]
root          29  0.0  0.0      0     0 ?        S    Feb16   0:00 [kdevtmpfs]
root          30  0.0  0.0      0     0 ?        I<   Feb16   0:00 [kworker/R-inet_frag_wq]
root          31  0.0  0.0      0     0 ?        I    Feb16   0:00 [rcu_tasks_kthread]
 [...]
```

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.

Protocol : LOCAL
```

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: 2026/02/03

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
```

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: 2026/02/03

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
  Version            : 8.18.0
  Associated Package : libcurl4t64

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
  Version            : 8.18.0
  Associated Package : libcurl3t64-gnutls
```

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: 2026/02/03

Plugin Output

tcp/0

```
  Path               : /usr/lib/x86_64-linux-gnu/libexiv2.so.0.28.7
  Version            : 0.28.7
  Associated Package : libexiv2-28 0.28.7
  Managed by OS      : True
```

136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

https://www.nginx.com

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2026/02/05

Plugin Output

tcp/0

```
Nessus detected 2 installs of nginx:

  Path    : nginx (via package manager)
  Version : 1.28.1-3

  Path               : /usr/sbin/nginx
  Version            : 1.28.1
  Associated Package : nginx: /usr/sbin/nginx
  Detection Method   : Binary in $PATH
  Full Version       : 1.28.1
  Managed by OS      : True
  Nginx Plus         : False
```