Localhost Scan

Report generated by Tenable Nessus™ Fri, 27 Jun 2025 08:01:49 EDT

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

190856 (1) - Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.19.1, 20.11.1, 21.6.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday February 14 2024 Security Releases advisory.

- On Linux, Node.js ignores certain environment variables if those may have been set by an unprivileged user while the process is running with elevated privileges with the only exception of CAP_NET_BIND_SERVICE. Due to a bug in the implementation of this exception, Node.js incorrectly applies this exception even when certain other capabilities have been set. This allows unprivileged users to inject code that inherits the process's elevated privileges. Impacts: Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21892)

- A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits. Impacts: Thank you, to Bartek Nowotarski for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2024-22019)

- The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer.from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21896)

- setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid().

This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). Impacts: Thank you, to valette for reporting this vulnerability and thank you Tobias Nieen for fixing it. (CVE-2024-22017)

- A vulnerability in the privateDecrypt() API of the crypto library, allowed a covert timing side-channel during PKCS#1 v1.5 padding error handling. The vulnerability revealed significant timing differences in decryption for valid and invalid ciphertexts. This poses a serious threat as attackers could remotely exploit the vulnerability to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing Json Web Encryption messages. Impacts: Thank you, to hkario for reporting this vulnerability and thank you Michael Dawson for fixing it. (CVE-2023-46809)

- Node.js depends on multiple built-in utility functions to normalize paths provided to node:fs functions, which can be overwritten with user-defined implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21891)

- The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: --allow-fs-read=/home/node/.ssh/*.pub will ignore pub and give access to everything after .ssh/. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21890)

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

See Also

http://www.nessus.org/u?313add11

Solution

Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.1041

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-46809
CVE	CVE-2024-21890
CVE	CVE-2024-21891
CVE	CVE-2024-21892
CVE	CVE-2024-21896
CVE	CVE-2024-22017
CVE	CVE-2024-22019
XREF	IAVB:2024-B-0016-S

Plugin Information

Published: 2024/02/21, Modified: 2025/04/03

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.11.1
```

185732 (1) - PostgreSQL 11.x < 11.22 / 12.x < 12.17 / 13.x < 13.13 / 14.x < 14.10 / 15.x < 15.5 / 16.x < 16.1 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities

Description

The version of PostgreSQL installed on the remote host is 11 prior to 11.22, 12 prior to 12.17, 13 prior to 13.13, 14 prior to 14.10, 15 prior to 15.5, or 16 prior to 16.1. As such, it is potentially affected by multiple vulnerabilities:

- Missing overflow checks let authenticated database users write arbitrary bytes to an area of memory that facilitates arbitrary code execution and read a wide area of server memory. (CVE-2023-5869)

- Certain aggregate function calls receiving an 'unknown'-type arguments can disclose bytes of server memory up to the next zero byte. (CVE-2023-5868)

- Role pg_cancel_backend can signal certain superuser processes contrary to the function documentation.

Examples of processes that could be improperly signaled are the logical replication launcher and the autovacuum launcher and workers. (CVE-2023-5870)

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

See Also

http://www.nessus.org/u?c84fe996

Solution

Upgrade to PostgreSQL 11.22 / 12.17 / 13.13 / 14.10 / 15.5 / 16.1 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0628

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5868
CVE	CVE-2023-5869
CVE	CVE-2023-5870
XREF	IAVB:2023-B-0088-S

Plugin Information

Published: 2023/11/15, Modified: 2025/05/29

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /opt/splunk/bin/postgres
Installed version : 16.0
Fixed version     : 16.1
```

192945 (1) - Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.1, 20.12.1, 21.7.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, April 3, 2024 Security Releases advisory.

- An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nghttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition. Impacts: Thank you, to bart for reporting this vulnerability and Anna Henningsen for fixing it. (CVE-2024-27983)

- The team has identified a vulnerability in the http server of the most recent version of Node, where malformed headers can lead to HTTP request smuggling. Specifically, if a space is placed before a content-length header, it is not interpreted correctly, enabling attackers to smuggle in a second request within the body of the first. Impacts: Thank you, to bpingel for reporting this vulnerability and Paolo Insogna for fixing it. Summary The Node.js project will release new versions of the 18.x, 20.x, 21.x releases lines on or shortly after, Wednesday, April 3, 2024 in order to address: (CVE-2024-27982)

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://nodejs.org/en/blog/vulnerability/april-2024-security-releases/

Solution

Upgrade to Node.js version 18.20.1 / 20.12.1 / 21.7.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.6865

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-27982
CVE	CVE-2024-27983
XREF	IAVB:2024-B-0033-S

Plugin Information

Published: 2024/04/05, Modified: 2024/04/19

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.12.1
```

201969 (1) - Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.4, 20.15.1, 22.4.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Monday, July 8, 2024 Security Releases advisory.

- The CVE-2024-27980 was identified as an incomplete fix for the BatBadBut vulnerability. This vulnerability arises from improper handling of batch files with all possible extensions on Windows via child_process.spawn / child_process.spawnSync. A malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled. This vulnerability affects all users of child_process.spawn and child_process.spawnSync on Windows in all active release lines.

Impact: Thank you, to tianst for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-27980)

- A security flaw in Node.js allows a bypass of network import restrictions. By embedding non-network imports in data URLs, an attacker can execute arbitrary code, compromising system security. Verified on various platforms, the vulnerability is mitigated by forbidding data URLs in network imports. Exploiting this flaw can violate network import security, posing a risk to developers and servers. Impact: Thank you, to dittyroma for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22020)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-write flag is used. Node.js Permission Model do not operate on file descriptors, however, operations such as fs.fchown or fs.fchmod can use a read-only file descriptor to change the owner and permissions of a file. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to 4xpl0r3r for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-36137)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-read flag is used. This flaw arises from an inadequate permission model that fails to restrict file stats through the fs.lstat API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to haxatron1 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22018)

- The Permission Model assumes that any path starting with two backslashes \ has a four-character prefix that can be ignored, which is not always true. This subtle bug leads to vulnerable edge cases. This vulnerability affects Windows users of the Node.js Permission Model in version v22.x and v20.x Impact:

Thank you, to tniessen for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-37372)

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://nodejs.org/en/blog/vulnerability/july-2024-security-releases/

Solution

Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0074

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-22018
CVE	CVE-2024-22020
CVE	CVE-2024-27980
CVE	CVE-2024-36137
CVE	CVE-2024-37372
XREF	IAVB:2024-B-0039-S

XREF IAVB:2024-B-0083-S

Plugin Information

Published: 2024/07/08, Modified: 2025/01/24

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.15.1
```

205594 (1) - PostgreSQL 12.x < 12.20 / 13.x < 13.16 / 14.x < 14.13 / 15.x < 15.8 / 16.x 16.4 SQL Injection<

Synopsis

The remote database server is affected by an SQL injection vulnerability

Description

The version of PostgreSQL installed on the remote host is 12 prior to 12.20, 13 prior to 13.16, 14 prior to 14.13, 15 prior to 15.8, or 16 prior to 16.4. As such, it is potentially affected by a vulnerability :

- Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction.

Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. (CVE-2024-7348)

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?6be9d6bf

http://www.nessus.org/u?5cdbab17

Solution

Upgrade to PostgreSQL 12.20 / 13.16 / 14.13 / 15.8 / 16.4 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0026

CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-7348
XREF	IAVB:2024-B-0117-S

Plugin Information

Published: 2024/08/15, Modified: 2025/05/29

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /opt/splunk/bin/postgres
Installed version : 16.0
Fixed version     : 16.4
```

211655 (1) - PostgreSQL 12.x < 12.21 / 13.x < 13.17 / 14.x < 14.14 / 15.x < 15.9 / 16.x < 16.5 / 17.x < 17.1 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities

Description

The version of PostgreSQL installed on the remote host is 12 prior to 12.21, 13 prior to 13.17, 14 prior to 14.14, 15 prior to 15.9, 16 prior to 16.5, or 17 prior to 17.1. As such, it is potentially affected by multiple vulnerabilities :

- Incorrect control of environment variables in PostgreSQL PL/Perl allows an unprivileged database user to change sensitive process environment variables (e.g. PATH). That often suffices to enable arbitrary code execution, even if the attacker lacks a database server operating system user. (CVE-2024-10979)

- Incorrect privilege assignment in PostgreSQL allows a less-privileged application user to view or change different rows from those intended. An attack requires the application to use SET ROLE, SET SESSION AUTHORIZATION, or an equivalent feature. The problem arises when an application query uses parameters from the attacker or conveys query results to the attacker. If that query reacts to current_setting('role') or the current user ID, it may modify or return data as though the session had not used SET ROLE or SET SESSION AUTHORIZATION. The attacker does not control which incorrect user ID applies. Query text from less-privileged sources is not a concern here, because SET ROLE and SET SESSION AUTHORIZATION are not sandboxes for unvetted queries. (CVE-2024-10978)

- Client use of server error message in PostgreSQL allows a server not trusted under current SSL or GSS settings to furnish arbitrary non-NUL bytes to the libpq application. For example, a man-in-the-middle attacker could send a long error message that a human or screen-scraper user of psql mistakes for valid query results. This is probably not a concern for clients where the user interface unambiguously indicates the boundary between one error message and other text. (CVE-2024-10977)

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

See Also

http://www.nessus.org/u?e9644dd1

Solution

Upgrade to PostgreSQL 13.17 / 14.14 / 15.9 / 16.5 / 17.1 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-10976
CVE	CVE-2024-10977
CVE	CVE-2024-10978
CVE	CVE-2024-10979
XREF	IAVB:2024-B-0175-S

Plugin Information

Published: 2024/11/20, Modified: 2025/05/29

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /opt/splunk/bin/postgres
Installed version : 16.0
Fixed version     : 16.5
```

214404 (1) - Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tuesday, January 21, 2025 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.6, 20.18.2, 22.13.1, 23.6.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Tuesday, January 21, 2025 Security Releases advisory.

- A memory leak could occur when a remote peer abruptly closes the socket without sending a GOAWAY notification. Additionally, if an invalid header was detected by nghttp2, causing the connection to be terminated by the peer, the same leak was triggered. This flaw could lead to increased memory consumption and potential denial of service under certain conditions. This vulnerability affects HTTP/2 Server users on Node.js v18.x, v20.x, v22.x and v23.x. Impact: Thank you, to newtmitch for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23085)

- With the aid of the diagnostics_channel utility, an event can be hooked into whenever a worker thread is created. This is not limited only to workers but also exposes internal workers, where an instance of them can be fetched, and its constructor can be grabbed and reinstated for malicious usage. This vulnerability affects Permission Model users (--permission) on Node.js v20, v22, and v23. Impact: Thank you, to leodog896 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23083)

- A vulnerability has been identified in Node.js, specifically affecting the handling of drive names in the Windows environment. Certain Node.js functions do not treat drive names as special on Windows. As a result, although Node.js assumes a relative path, it actually refers to the root directory. On Windows, a path that does not start with the file separator is treated as relative to the current directory. This vulnerability affects Windows users of path.join API. Impact: Thank you, to taise for reporting this vulnerability and thank you tniessen for fixing it. (CVE-2025-23084)

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

See Also

http://www.nessus.org/u?68bc9901

Solution

Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-23083
CVE	CVE-2025-23084
CVE	CVE-2025-23085
XREF	IAVB:2025-B-0012-S

Plugin Information

Published: 2025/01/21, Modified: 2025/05/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.18.2
```

216586 (1) - PostgreSQL 13.x < 13.19 / 14.x < 14.16 / 15.x < 15.11 / 16.x < 16.7 / 17.x < 17.3 SQLi

Synopsis

The remote database server is affected by a vulnerability

Description

The version of PostgreSQL installed on the remote host is 13 prior to 13.19, 14 prior to 14.16, 15 prior to 15.11, 16 prior to 16.7, or 17 prior to 17.3. As such, it is potentially affected by a vulnerability :

- Improper neutralization of quoting syntax in PostgreSQL libpq functions PQescapeLiteral(), PQescapeIdentifier(), PQescapeString(), and PQescapeStringConn() allows a database input provider to achieve SQL injection in certain usage patterns. Specifically, SQL injection requires the application to use the function result to construct input to psql, the PostgreSQL interactive terminal. Similarly, improper neutralization of quoting syntax in PostgreSQL command line utility programs allows a source of command line arguments to achieve SQL injection when client_encoding is BIG5 and server_encoding is one of EUC_TW or MULE_INTERNAL. Versions before PostgreSQL 17.3, 16.7, 15.11, 14.16, and 13.19 are affected.

(CVE-2025-1094)

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?2a3cbcdf

Solution

Upgrade to PostgreSQL 13.19 / 14.16 / 15.11 / 16.7 / 17.3 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

9.5

EPSS Score

0.8363

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2025-1094
XREF	IAVB:2025-B-0028-S

Exploitable With

Metasploit (true)

Plugin Information

Published: 2025/02/21, Modified: 2025/05/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /opt/splunk/bin/postgres
Installed version : 16.0
Fixed version     : 16.7
```

237199 (1) - Python Library Tornado 6.5.0 DoS

Synopsis

A Python library installed on the remote host is affected by a DoS vulnerability.

Description

The detected version of the Tornado Python package, Tornado, is prior to 6.4.2.

It is therefore affected by a DoS vulnerability that happens When Tornado's multipart/form-data parser encounters certain errors, it logs a warning but continues trying to parse the remainder of the data. This allows remote attackers to generate an extremely high volume of logs, constituting a DoS attack. This DoS is compounded by the fact that the logging subsystem is synchronous.:

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?5105fc6c

Solution

Upgrade to Tornado version 6.5.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-47287

Plugin Information

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

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Installed version : 6.4.2
Fixed version     : 6.5.0
```

51192 (1) - 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

192.168.235.131 (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
```

197741 (1) - PostgreSQL 14.x < 14.12 / 15.x < 15.7 / 16.x < 16.3 Missing Authorization Check

Synopsis

The remote database server is affected by a vulnerability

Description

The version of PostgreSQL installed on the remote host is 14 prior to 14.12, 15 prior to 15.7, or 16 prior to 16.3. As such, it is potentially affected by a vulnerability :

- Missing authorization in PostgreSQL built-in views pg_stats_ext and pg_stats_ext_exprs allows an unprivileged database user to read most common values and other statistics from CREATE STATISTICS commands of other users. The most common values may reveal column values the eavesdropper could not otherwise read or results of functions they cannot execute. Installing an unaffected version only fixes fresh PostgreSQL installations, namely those that are created with the initdb utility after installing that version. Current PostgreSQL installations will remain vulnerable until they follow the instructions in the release notes. Within major versions 14-16, minor versions before PostgreSQL 16.3, 15.7, and 14.12 are affected. Versions before PostgreSQL 14 are unaffected. (CVE-2024-4317)

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?07fc5d58

http://www.nessus.org/u?1940556a

Solution

Upgrade to PostgreSQL 14.12 / 15.7 / 16.3 or later

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-4317
XREF	IAVB:2024-B-0062-S

Plugin Information

Published: 2024/05/23, Modified: 2025/05/29

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /opt/splunk/bin/postgres
Installed version : 16.0
Fixed version     : 16.3
```

236766 (1) - Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vulnerabilities (Wednesday, May 14, 2025 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 20.19.2, 22.15.1, 22.15.1, 23.11.1, 24.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, May 14, 2025 Security Releases advisory.

- In Node.js, the ReadFileUtf8 internal binding leaks memory due to a corrupted pointer in uv_fs_s.file: a UTF-16 path buffer is allocated but subsequently overwritten when the file descriptor is set. This results in an unrecoverable memory leak on every call. Repeated use can cause unbounded memory growth, leading to a denial of service. Impact: Thank you, to Justin Nietzel for reporting and fixing this vulnerability.

(CVE-2025-23165)

- The C++ method SignTraits::DeriveBits() may incorrectly call ThrowException() based on user-supplied inputs when executing in a background thread, crashing the Node.js process. Such cryptographic operations are commonly applied to untrusted inputs. Thus, this mechanism potentially allows an adversary to remotely crash a Node.js runtime. Impact: Thank you, @panva and @tniessen, for reporting and fixing this vulnerability. (CVE-2025-23166)

- A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r \rX instead of the required \r \r . This inconsistency enables request smuggling, allowing attackers to bypass proxy- based access controls and submit unauthorized requests. The issue was resolved by upgrading llhttp to version 9, which enforces correct header termination. Impact: Thank you, to kenballus for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23167)

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://nodejs.org/en/blog/vulnerability/may-2025-security-releases/

Solution

Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-23165
CVE	CVE-2025-23166
CVE	CVE-2025-23167
XREF	IAVB:2025-B-0079

Plugin Information

Published: 2025/05/15, Modified: 2025/05/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.19.2
```

148373 (3) - 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: 2025/02/12

Plugin Output

192.168.235.131 (tcp/0)

```
Path            : /usr/lib/jvm/java-11-openjdk-amd64/
Version         : Unknown
Binary Location : /usr/lib/jvm/java-11-openjdk-amd64/bin/java
Managed by OS   : True
```

192.168.235.131 (tcp/0)

```
Path            : /usr/lib/jvm/java-17-openjdk-amd64/
Version         : 17.0.15
Binary Location : /usr/lib/jvm/java-17-openjdk-amd64/bin/java
Managed by OS   : True
```

192.168.235.131 (tcp/0)

```
Path            : /usr/lib/jvm/java-21-openjdk-amd64/
Version         : 21.0.7
Binary Location : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Managed by OS   : True
```

22964 (2) - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.235.131 (tcp/8834/www)

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

192.168.235.131 (tcp/8834/www)

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

130024 (2) - PostgreSQL Client/Server Installed (Linux)

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/10/18, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of PostgreSQL client:

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

  Path    : /opt/splunk/bin/psql
  Version : 16.0
```

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of PostgreSQL:

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

  Path    : /opt/splunk/bin/postgres
  Version : 16.0
```

10107 (1) - 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

192.168.235.131 (tcp/8834/www)

```
The remote web server type is :

NessusWWW
```

10147 (1) - 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: 2023/02/08

Plugin Output

192.168.235.131 (tcp/8834/www)

```
URL     : https://192.168.235.131:8834/
Version : unknown
```

10863 (1) - 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

192.168.235.131 (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: 00 8A 97

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 27 10:31:54 2025 GMT
Not Valid After: Jun 26 10:31:54 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
```

```
Public Key: 00 C7 51 92 DF 0F ED 4B D8 DD 7E C4 0B DC 9C 27 5B A9 49 1A
            B1 CC A4 FF FF EF C1 1C 22 AF E6 4D 85 36 B1 C7 CD 5B 6E F4
            DC 8F 76 96 DF 64 BE 88 DE F7 EA 46 8E D0 EF 0F 06 66 41 20
            75 C1 39 79 14 35 21 71 DD 2F EE FF BE 8D 2B 94 C3 AB 7C F3
            2C 8A BC 0C F7 27 4F CA A4 17 D4 DC 07 F6 1A 12 C7 EF E6 77
            AD 26 25 71 CE BE 39 26 A3 15 3D F0 7E 0F AD 8B CC 5C DE 37
            36 66 FA 2A 33 FC 14 4C 15 27 EC 7D 81 AF 7A C0 6C EF 9C 24
            2E D7 98 7C EB A4 6D AD 84 41 3B 4E 4C DD 5A 25 7C 43 B7 34
            F7 B5 62 6D 82 75 A2 C6 1A E9 98 3C 06 14 5A 29 6E 2F 06 57
            C0 9D EB 3A 2A B9 1A 46 17 B6 EA 15 AE 2E C8 66 C5 24 7F 47
            03 7B 79 84 08 FA 9C A7 FB EF 80 32 B9 E9 41 67 9B C6 E1 EC
            76 73 5C 11 30 D1 43 C3 37 52 43 B3 3E 8A E9 D7 84 8D B3 1B
            86 8E 4E 63 23 E1 A2 8D AA 89 3F 75 85 FC 22 F6 93
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 0A BD 35 E0 C4 99 1A 2B DD 24 D9 55 0B F7 9E 5B 75 4A AD
           D1 30 9F 9C F6 47 61 D6 1E 98 A3 47 F8 B1 A6 81 76 43 2A 5D
           3E 9B 65 9D 99 1B 4B 70 29 9D 4B 98 71 59 4C DA 29 BA 3F 2E
           67 54 95 3D F6 D9 73 53 6E E1 80 AA 68 A1 FC B4 E7 71 5C 23
           DD 5F C2 D8 0B 50 C1 E8 91 71 FC 6F 82 A9 F1 40 60 C6 5E EE
           83 CC 0F AA 5B 04 81 B4 2E AB 60 DC CA 81 9A DC 1A 27 10 CE
           8C 83 72 E9 73 54  [...]
```

11936 (1) - 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

192.168.235.131 (tcp/0)

```
Remote operating system : Linux Kernel 6.12.25-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.12.25-amd64
```

14272 (1) - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

192.168.235.131 (tcp/8834/www)

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

19506 (1) - 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: 2025/06/25

Plugin Output

192.168.235.131 (tcp/0)

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202506270156
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
```

```
Scan name :  Localhost Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.235.131
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 : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/6/27 7:45 EDT (UTC -04:00)
Scan duration : 984 sec
Scan for malware : no
```

20094 (1) - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

192.168.235.131 (tcp/0)

```
The remote host is a VMware virtual machine.
```

21643 (1) - 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

192.168.235.131 (tcp/8834/www)

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

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

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


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

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ----------------------  ---
```

```
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH           RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH           RSA      AES-GCM(256)
 SHA384

The fields above are :

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

22869 (1) - 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

192.168.235.131 (tcp/0)

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

  ii   7zip  24.09+dfsg-8  amd64  7-Zip file archiver with a high compression ratio
  ii   accountsservice  23.13.9-7  amd64  query and manipulate user account information
  ii   acl  2.3.2-2+b1  amd64  access control list - utilities
  ii   adduser  3.152  all  add and remove users and groups
  ii   adwaita-icon-theme  48.0-1  all  default icon theme of GNOME
  ii   aircrack-ng  1:1.7+git20230807.4bf83f1a-2  amd64  wireless WEP/WPA cracking utilities
  ii   alsa-topology-conf  1.2.5.1-3  all  ALSA topology configuration files
  ii   alsa-ucm-conf  1.2.14-1  all  ALSA Use Case Manager configuration files
  ii   amass  4.2.0-0kali1  amd64  In-depth DNS Enumeration and Network Mapping
  ii   amass-common  4.2.0-0kali1  all  In-depth DNS Enumeration and Network Mapping
  ii   amd64-microcode  3.20250311.1  amd64  Platform firmware and microcode for AMD CPUs and SoCs
  ii   apache2  2.4.63-1  amd64  Apache HTTP Server
  ii   apache2-bin  2.4.63-1  amd64  Apache HTTP Server (modules and other binary files)
  ii   apache2-data  2.4.63-1  all  Apache HTTP Server (common files)
  ii   apache2-utils  2.4.63-1  amd64  Apache HTTP Server (utility programs for web servers)
  ii   apparmor  4.1.0-1  amd64  user-space parser utility for AppArmor
  ii   apt  3.0.2+kali1  amd64  commandline package manager
  ii   apt-file  3.3  all  search for files within Debian packages (command-line interface)
  ii   apt-transport-https  3.0.2+kali1  all  transitional package for https support
```

```
ii   apt-utils  3.0.2+kali1  amd64  package management related utility programs
ii   arj  3.10.22-28  amd64  archiver for .arj files
ii   arp-scan  1.10.0-2+b1  amd64  arp scanning and fingerprinting tool
ii   arping  2.25-1  amd64  sends IP and/or ARP pings (to the MAC address)
ii   aspell  0.60.8.1-4  amd64  GNU Aspell spell-checker
ii   aspell-en  2020.12.07-0-1  all  English dictionary for GNU Aspell
ii   aspnetcore-runtime-6.0  6.0.8-1  amd64
ii   aspnetcore [...]
```

24260 (1) - 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

192.168.235.131 (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: 648f9856fb742fd1ad80a4e90e544995
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Fri, 27 Jun 2025 11:45:43 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=1744138425399" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=0e2ae10949ed6782467b3810ccce69c5" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1744138425399"></script>
        <script src="p [...]
```

25202 (1) - Enumerate IPv6 Interfaces via SSH

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.235.131 (tcp/0)

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

 - fe80::8474:2b2f:d150:4ce1 (on interface eth0)
 - ::1 (on interface lo)
```

25203 (1) - Enumerate IPv4 Interfaces via SSH

Synopsis

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

Description

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

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.235.131 (tcp/0)

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

 - 172.17.0.1 (on interface docker0)
 - 192.168.235.131 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

33276 (1) - 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

192.168.235.131 (tcp/0)

```
The following MAC addresses exist on the remote host :

  - 02:42:94:72:36:09 (interface docker0)
  - 00:0c:29:cb:1a:4a (interface eth0)
```

35716 (1) - 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

192.168.235.131 (tcp/0)

```
The following card manufacturers were identified :

00:0C:29:CB:1A:4A : VMware, Inc.
```

42822 (1) - 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

192.168.235.131 (tcp/8834/www)

```
The STS header line is :

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

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.235.131 (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:2.4.63 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:log4j:2.17.2 -> Apache Software Foundation log4j
  cpe:/a:apache:log4j:2.24.3 -> Apache Software Foundation log4j
  cpe:/a:docker:docker:1 -> Docker
  cpe:/a:exiv2:exiv2:0.28.5 -> Exiv2
  cpe:/a:exiv2:libexiv2:0.28.5
  cpe:/a:gnupg:libgcrypt:1.11.0 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:8.14.1 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.14.1 -> Haxx libcurl
  cpe:/a:haxx:libcurl:8.5.0 -> Haxx libcurl
  cpe:/a:jmcnamara:spreadsheet%3a%3aparseexcel:0.66 -> John McNamara Spreadsheet::ParseExcel
```

```
cpe:/a:linuxfoundation:containerd:1.7.24 -> The Linux Foundation containerd
cpe:/a:nginx:nginx:1.26.3 -> Nginx
cpe:/a:nginx:nginx:1.26.3-3 -> Nginx
cpe:/a:nodejs:node.js:20.11.0 -> Nodejs Node.js
cpe:/a:nodejs:node.js:20.19.2 -> Nodejs Node.js
cpe:/a:numpy:numpy:2.2.4 -> NumPy
cpe:/a:openssl:openssl:1.0.2zk -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.0.15 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.4.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.5.0 -> OpenSSL Project OpenSSL
cpe:/a:openvpn:openvpn:2.6.14 -> OpenVPN
cpe:/a:oracle:openjdk:17.0.15 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:21.0.7 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:unknown -> Oracle OpenJDK -
cpe:/a:php:php:8.2.27 -> PHP PHP
cpe:/a:postgresql:postgresql:16.0 -> PostgreSQL
cpe:/a:postgresql:postgresql:17.5 -> PostgreSQL
cpe:/a:ruby-lang:ruby:3.3.8 -> Ruby-lang Ruby
cpe:/a:splunk:splunk:9.4.1 -> Splunk
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tenable:nessus -> Tenable Nessus
cpe:/a:tenable:nessus:10.8.4 -> Tenable Nessus
cpe:/a:tornadoweb:tornado:6.4.2 -> Tornado Web Server Tornado
cpe:/a:tukaani:xz:5.8.1 -> Tukaani XZ
cpe:/a:vim:vim:9.1 -> Vim
cpe:/a:vmware:open_vm_tools:12.5.0 -> VMware Open VM Tools
cpe:/a:wazuh:wazuh:4.12.0 -> Wa [...]
```

54615 (1) - 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

192.168.235.131 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 99
```

55472 (1) - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/06/23

Plugin Output

192.168.235.131 (tcp/0)

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

56468 (1) - 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

192.168.235.131 (tcp/0)

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

56984 (1) - 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

192.168.235.131 (tcp/8834/www)

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

57041 (1) - 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

192.168.235.131 (tcp/8834/www)

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

  High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

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

64582 (1) - 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

192.168.235.131 (tcp/0)

66334 (1) - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/06/10

Plugin Output

192.168.235.131 (tcp/0)

```
. You need to take the following 3 actions :


[ Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple
 Vulnerabilities (Wednesday, May 14, 2025 Security Releases). (236766) ]

+ Action to take : Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or
 later.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).


[ PostgreSQL 13.x < 13.19 / 14.x < 14.16 / 15.x < 15.11 / 16.x < 16.7 / 17.x < 17.3 SQLi (216586) ]

+ Action to take : Upgrade to PostgreSQL 13.19 / 14.16 / 15.11 / 16.7 / 17.3 or later

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).


[ Python Library Tornado 6.5.0 DoS (237199) ]

+ Action to take : Upgrade to Tornado version 6.5.0 or later.
```

86420 (1) - 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

192.168.235.131 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 02:42:94:72:36:09
  - 00:0C:29:CB:1A:4A
```

93561 (1) - Docker Service Detection

Synopsis

Docker was detected on the remote host.

Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

See Also

https://www.docker.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/09/16, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Client:
Server:
  Version: 0.19.0


There were no containers detected running on Docker.
```

95928 (1) - 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

192.168.235.131 (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
               cdrom
               adm
               audio
               sudo
               kaboxer
               bluetooth
               plugdev
               floppy

User         : splunk
Home folder  : /opt/splunk
Start script : /bin/bash
Groups       : splunk
```

```
----------[ 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  : / [...]
```

97993 (1) - 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

192.168.235.131 (tcp/0)

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

The output of "uname -a" is :
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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 : 3.384043 seconds
```

110095 (1) - 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: 2024/03/25

Plugin Output

192.168.235.131 (tcp/0)

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

110483 (1) - 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

192.168.235.131 (tcp/0)

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.1  24216 14620 ?        Ss   06:08   0:06 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    06:08   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    06:08   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-sync_wq]
root           7  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-slub_flushwq]
root           8  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-netns]
root          10  0.0  0.0      0     0 ?        I    06:08   0:02 [kworker/0:1-events]
root          12  0.0  0.0      0     0 ?        I    06:08   0:00 [kworker/u128:0-ipv6_addrconf]
root          13  0.0  0.0      0     0 ?        I<   06:08   0:00 [kworker/R-mm_percpu_wq]
root          14  0.0  0.0      0     0 ?        I    06:08   0:00 [rcu_tasks_kthread]
root          15  0.0  0.0      0     0 ?        I    06:08   0:00 [rcu_tasks_rude_kthread]
root          16  0.0  0.0      0     0 ?        I    06:08   0:00 [rcu_tasks_trace_kthread]
root          17  0.0  0.0      0     0 ?        S    06:08   0:01 [ksoftirqd/0]
root          18  0.0  0.0      0     0 ?        I    06:08   0:04 [rcu_preempt]
root          19  0.0  0.0      0     0 ?        S    06:08   0:00 [rcu_exp_par_gp_kthread_worker/1]
root          20  0.0  0.0      0     0 ?        S    06:08   0:00 [rcu_exp_gp_kthread_worker]
root          21  0.0  0.0      0     0 ?        S    06:08   0:00 [migration/0]
root          22  0.0  0.0      0     0 ?        S    06:08   0:00 [idle_inject/0]
root          23  0.0  0.0      0     0 ?        S    06:08   0:00 [cpuhp/0]
root          24  0.0  0.0      0     0 ?        S    06:08   0:00 [cpuhp/1]
root          25  0.0  0.0      0     0 ?      [...]
```

117887 (1) - 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

192.168.235.131 (tcp/0)

```
OS Security Patch Assessment is available.

Protocol : LOCAL
```

136318 (1) - 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

192.168.235.131 (tcp/8834/www)

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

136340 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of nginx:

  Path    : nginx (via package manager)
  Version : 1.26.3-3

  Path               : /usr/sbin/nginx
  Version            : 1.26.3
  Associated Package : nginx: /usr/sbin/nginx
  Detection Method   : Binary in $PATH
  Full Version       : 1.26.3
  Managed by OS      : True
  Nginx Plus         : False
```

138330 (1) - 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

192.168.235.131 (tcp/8834/www)

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

141118 (1) - 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

192.168.235.131 (tcp/0)

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

141394 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/sbin/apache2
Version            : 2.4.63
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS      : True
Running            : no

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

Loaded modules :
  - 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_event
      - mod_negotiation
      - mod_reqtimeout
      - mod_setenvif
      - mod_status
```

142640 (1) - 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: 2025/02/12

Plugin Output

192.168.235.131 (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
```

147817 (1) - Java Detection and Identification (Linux / Unix)

Synopsis

Java is installed on the remote Linux / Unix host.

Description

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

Notes:

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

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

See Also

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 3 installs of Java:

  Path             : /usr/lib/jvm/java-11-openjdk-amd64/
  Version          : Unknown
  Application      : OpenJDK Java
  Binary Location  : /usr/lib/jvm/java-11-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

  Path             : /usr/lib/jvm/java-17-openjdk-amd64/
  Version          : 17.0.15
  Application      : OpenJDK Java
  Binary Location  : /usr/lib/jvm/java-17-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

  Path             : /usr/lib/jvm/java-21-openjdk-amd64/
  Version          : 21.0.7
  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
```

151883 (1) - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 4 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
  Version : 1.11.0

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.0

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
  Version : 1.11.0

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.0
```

152742 (1) - 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

192.168.235.131 (tcp/0)

```
Unix software discovery checks are available.

Protocol : LOCAL
```

156000 (1) - 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.

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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 3 installs of Apache Log4j:

  Path                           : /opt/splunk/etc/apps/splunk_archiver/java-bin/jars/thirdparty/
common/log4j-core-2.17.2.jar
  Version                        : 2.17.2
  JMSAppender.class association  : Found
  JdbcAppender.class association : Found
  JndiLookup.class association   : Found
  Method                         : log4j-core file search
```

```
Path                            : /usr/share/zaproxy/lib/log4j-core-2.24.3.jar
Version                         : 2.24.3
JMSAppender.class association   : Found
JdbcAppender.class association  : Found
JndiLookup.class association    : Found
Method                          : log4j-core file search

Path                            : /opt/splunk/bin/jars/thirdparty/common/log4j-core-2.17.2.jar
Version                         : 2.17.2
JMSAppender.class association   : Found
JdbcAppender.class association  : Found
JndiLookup.class association    : Found
Method                          : log4j-core file search
```

157358 (1) - 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

192.168.235.131 (tcp/0)

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            6.8G     0  6.8G   0% /dev
tmpfs           1.4G  1.3M  1.4G   1% /run
/dev/sda1        79G   48G   28G  64% /
tmpfs           6.8G  8.0K  6.8G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           6.8G   84K  6.8G   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           1.4G  4.1M  1.4G   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 /


$ 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=7050328k,nr_inodes=1762582,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=1423640k,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)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
 (rw,relatime,fd=40,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=6746)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,nosuid,nodev,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
tmpfs on /run/credential [...]
```

159273 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Dockerfiles found: 12
 - /home/kali/.cache/Cypress/13.17.0/Cypress/resources/app/node_modules/getos/Dockerfile
 - /home/kali/juice-shop/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/alpine/3.3/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/debian/7.3/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/debian/7.4/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/debian/7.5/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/debian/7.6/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/fedora/20/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/ubuntu/13.10/Dockerfile
 - /home/kali/juice-shop/node_modules/getos/tests/ubuntu/14.04/Dockerfile
 - /home/kali/juice-shop/test/smoke/Dockerfile
```

159488 (1) - Docker Installed (Linux)

Synopsis

Docker was detected on the remote host.

Description

A container virtualization suite is installed on the remote host.

See Also

https://www.docker.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/04/04, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path          : /usr/bin/docker
Version       : 1
Build         : 411e817
Managed by OS : True
```

163326 (1) - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path    : /opt/nessus
Version : 10.8.4
Build   : 20028
```

163460 (1) - Splunk Installed (Linux)

Synopsis

Splunk was detected on the remote Linux host.

Description

Splunk was detected on the remote Linux host.

See Also

https://www.splunk.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/26, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path          : /opt/splunk
Version       : 9.4.1
License       : Enterprise
Trial License : Yes
```

168007 (1) - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

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

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

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

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 8 installs of OpenSSL:

  Path               : /usr/bin/openssl
  Version            : 3.5.0
  Associated Package : openssl 3.5.0-2
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
  Version            : 3.4.0
  Associated Package : libruby3.1t64
```

```
  Path               : /opt/nessus/bin/openssl
  Version            : 3.0.15
  Associated Package : nessus

  Path               : /opt/splunk/lib/libssl.so.1.0.0
  Version            : 1.0.2zk
  Associated Package : splunk

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

  Path               : /opt/splunk/lib/libcrypto.so.1.0.0
  Version            : 1.0.2zk
  Associated Package : splunk

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Version            : 3.5.0
  Associated Package : libssl3t64

  Path               : /opt/splunk/bin/openssl
  Version            : 1.0.2zk
  Associated Package : splunk

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
```

168980 (1) - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

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

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/06/23

Plugin Output

192.168.235.131 (tcp/0)

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

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

168982 (1) - 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

192.168.235.131 (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:

/home/kali/juice-shop/node_modules/@types/config
/usr/share/node_modules/@babel/core/lib/config
/usr/share/node_modules/@babel/eslint-shared-fixtures/config
/usr/share/node_modules/@babel/generator/lib/node
/usr/share/node_modules/@babel/helper-define-polyfill-provider/lib/node
/usr/share/node_modules/@babel/node
/usr/share/node_modules/@npmcli/config
/usr/share/node_modules/@types/node
/usr/share/nodejs/@babel/core/lib/config
/usr/share/nodejs/@babel/eslint-shared-fixtures/config
/usr/share/nodejs/@babel/generator/lib/node
/usr/share/nodejs/@babel/helper-define-polyfill-provider/lib/node
/usr/share/nodejs/@babel/node
/usr/share/nodejs/@npmcli/config
/usr/share/nodejs/@types/node
```

170170 (1) - 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

192.168.235.131 (tcp/0)

```
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
      ScopeID : 0x10
docker0:
  MAC : 02:42:94:72:36:09
  IPv4:
    - Address : 172.17.0.1
      Netmask : 255.255.0.0
      Broadcast : 172.17.255.255
eth0:
  MAC : 00:0c:29:cb:1a:4a
  IPv4:
    - Address : 192.168.235.131
      Netmask : 255.255.255.0
      Broadcast : 192.168.235.255
  IPv6:
    - Address : fe80::8474:2b2f:d150:4ce1
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
```

171410 (1) - IP Assignment Method Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/06/23

Plugin Output

192.168.235.131 (tcp/0)

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eth0
  + IPv4
    - Address       : 192.168.235.131
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::8474:2b2f:d150:4ce1
      Assign Method : static
+ docker0
  + IPv4
    - Address       : 172.17.0.1
      Assign Method : static
```

174788 (1) - SQLite Local Detection (Linux)

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, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

https://www.sqlite.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/26, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of SQLite:

  Path    : /usr/bin/sqlite3
  Version : unknown

  Path    : /bin/sqlite3
  Version : unknown
```

178771 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of Node.js:

  Path    : /usr/lib/python3/dist-packages/playwright/driver/node
  Version : 20.11.0

  Path            : /usr/bin/node
  Version         : 20.19.2
  Managed         : 1
  Package         : nodejs
  Package release : 1
  Package version : 20.19.2+dfsg

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

178772 (1) - Node.js Modules Installed (Linux)

Synopsis

Nessus was able to enumerate one or more Node.js modules installed on the remote host.

Description

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

See Also

https://nodejs.org/api/modules.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/07/25, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Installed top-level Node.js modules :

name: fs-minipass
version: 3.0.3
path: /usr/share/nodejs/tar/node_modules/fs-minipass/package.json

name: npm-install-checks
version: 6.0.0
path: /usr/share/nodejs/libnpmaccess/node_modules/npm-install-checks/package.json

name: treeverse
version: 3.0.0
path: /usr/share/nodejs/libnpmaccess/node_modules/treeverse/package.json

name: socks-proxy-agent
version: 7.0.0
path: /usr/share/nodejs/libnpmaccess/node_modules/socks-proxy-agent/package.json

name: npm-profile
version: 7.0.1
path: /usr/share/nodejs/libnpmaccess/node_modules/npm-profile/package.json
```

```
name: init-package-json
version: 4.0.1
path: /usr/share/nodejs/libnpmaccess/node_modules/init-package-json/package.json

name: process
version: 0.11.10
path: /usr/share/nodejs/libnpmaccess/node_modules/process/package.json

name: is-lambda
version: 1.0.1
path: /usr/share/nodejs/libnpmaccess/node_modules/is-lambda/package.json

name: fastest-levenshtein
version: 1.0.16
path: /usr/share/nodejs/libnpmaccess/node_modules/fastest-levenshtein/package.json

name: abort-controller
version: 3.0.0
path: /usr/share/nodejs/libnpmaccess/node_modules/abort-controller/package.json

name: parse-conflict-json
version: 3.0.0
path: /usr/share/nodejs/libnpmaccess/node_modules/parse-conflict-json/package.json

name: npm-pick-manifest
version: 8.0.1
path: /usr/share/nodejs/libnpmaccess/node_modules/npm-pick-manifest/package.json

name: read-package-json-fast
version: 3.0.1
path: /usr/share/nodejs/libnpmaccess/node_modules/read-package-json-fast/package.json

name: just-diff
version: 5.1.1
path: /usr/share/nodejs/libnpmaccess/node_modules/just-diff/package.json

name: socks
version: 2.7.0
path: /usr/share/nodejs/libnpmaccess/node_modules/socks/package.json

name: json-stringify-nice
version: 1.1.4
path: /usr/share/nodejs/libnpmaccess/node_modules/json-stringify-nice/package.json

name: agentkeepalive
version: 4.2.1
path: /usr/share/nodejs/libnpmaccess/node_modules/agentkeepalive/package.json

name: cidr-regex
version: 3.1.1
path: /usr/share/nodejs/l [...]
```

179139 (1) - 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

192.168.235.131 (tcp/0)

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

179200 (1) - 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

192.168.235.131 (tcp/0)

```
Gateway Routes:
  eth0:
    ipv4_gateways:
      192.168.235.2:
        subnets:
          - 0.0.0.0/0
Interface Routes:
  docker0:
    ipv4_subnets:
      - 172.17.0.0/16
  eth0:
    ipv4_subnets:
      - 192.168.235.0/24
    ipv6_subnets:
      - fe80::/64
```

182774 (1) - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

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

Additional information:

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

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

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

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/bin/curl
Version            : 8.14.1
Associated Package : curl 8.14.1-1
Managed by OS      : True
```

182848 (1) - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

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

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

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

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 3 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
  Version            : 8.14.1
  Associated Package : libcurl4t64

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
  Version            : 8.14.1
  Associated Package : libcurl3t64-gnutls
```

```
  Path               : /opt/splunk/opt/mongo/lib/libcurl.so.4.8.0
  Version            : 8.5.0
  Associated Package : splunk
```

186361 (1) - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

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

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path    : /usr/bin/vmtoolsd
Version : 12.5.0
```

189731 (1) - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of Vim:

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

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

189990 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (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
```

192709 (1) - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

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

Description

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

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.8.1
  Version            : 5.8.1
  Associated Package : liblzma5 5.8.1-1
```

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

Path               : /usr/bin/xz
Version            : 5.8.1
Associated Package : xz-utils 5.8.1-1
Confidence         : High
Managed by OS      : True
Version Source     : Package
```

193143 (1) - 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

192.168.235.131 (tcp/0)

```
Via date: EDT -0400
Via timedatectl: Time zone: America/New_York (EDT, -0400)
Via /etc/timezone: America/New_York
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

200214 (1) - 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: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path          : libndp0 1.9-1 (via package manager)
Version       : 1.9
Managed by OS : True
```

202184 (1) - Ruby Programming Language Installed (Linux)

Synopsis

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

Description

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

See Also

https://ruby.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/11, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

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

204827 (1) - Exiv2 Installed (Linux / Unix)

Synopsis

Exiv2 is installed on the remote Linux / Unix host.

Description

Exiv2 is installed on the remote Linux / Unix host.

Additional information:

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

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

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/bin/exiv2
Version            : 0.28.5
Associated Package : exiv2 0.28.5
Managed by OS      : True
```

204828 (1) - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

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

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

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/lib/x86_64-linux-gnu/libexiv2.so.0.28.5
Version            : 0.28.5
Associated Package : libexiv2-28 0.28.5
Managed by OS      : True
```

209654 (1) - 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

192.168.235.131 (tcp/0)

```
Following OS Fingerprints were found

Remote operating system : Linux Kernel 6.12.25-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30)
 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
d778302294b9cae0094e819ba2d7d19603e70af1
```

216936 (1) - PHP Scripting Language Installed (Unix)

Synopsis

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

Description

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

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

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/bin/php8.2
Version            : 8.2.27
Associated Package : php8.2-cli: /usr/bin/php8.2
INI file           : /etc/php/8.2/cli/php.ini
INI source         : PHP binary grep
Managed by OS      : True
```

232856 (1) - OpenVPN Installed (Linux)

Synopsis

OpenVPN is installed on the remote Linux host.

Description

OpenVPN is installed on the remote Linux host.

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

See Also

https://openvpn.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/19, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

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

235055 (1) - Wazuh Server Installed (Linux / UNIX)

Synopsis

Wazuh Server is installed on the remote Linux / UNIX host.

Description

Wazuh Server is installed on the remote Linux / UNIX host.

See Also

http://www.nessus.org/u?f5d1731f

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/01, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path    : /var/ossec/bin/wazuh-control
Version : 4.12.0
```

237200 (1) - 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: 2025/06/23

Plugin Output

192.168.235.131 (tcp/0)

```
Path    : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Version : 6.4.2
```

237414 (1) - Containerd Installed (Linux)

Synopsis

containerd was detected on the remote host.

Description

containerd, a container runtime which can manage the complete container lifecycle of its host system is installed on the target host.

See Also

https://github.com/containerd/containerd/tree/main

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/28, Modified: 2025/06/16

Plugin Output

192.168.235.131 (tcp/0)

```
Path               : /usr/bin/containerd
Version            : 1.7.24
Associated Package : containerd 1.7.24
Managed by OS      : True
```