tenable Nessus

Report generated by Tenable Nessus™

BlueMoon

Sat, 15 Nov 2025 16:48:57 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.136.108.235

CRITICAL	HIGH	MEDIUM	LOW	INFO
11	59	60	3	66

Scan Information

Start time:	Sat Nov 15 16:41:56 2025
End time:	Sat Nov 15 16:48:56 2025

Host Information

IP:	10.136.108.235
MAC Address:	08:00:27:43:85:F4 02:42:3A:28:DE:BC
OS:	Linux Kernel 4.19.0-14-amd64 on Debian 10.8

Vulnerabilities

161329 - Debian DSA-5139-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5139 advisory.

Elison Niven discovered that the c_rehash script included in OpenSSL did not sanitise shell meta characters which could result in the execution of arbitrary commands. For the oldstable distribution (buster), this problem has been fixed in version 1.1.1n-0+deb10u2. For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u2. We recommend that you upgrade your openssl packages. For the detailed security status of openssl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/security/2022/dsa-5139
https://security-tracker.debian.org/tracker/CVE-2022-1292
https://packages.debian.org/source/buster/openssl
https://packages.debian.org/source/bullseye/openssl

Solution

Upgrade the openssl packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u2.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

STIG Severity

I

References

CVE	CVE-2022-1292
XREF	IAVA:2022-A-0186-S

Plugin Information

Published: 2022/05/18, Modified: 2025/08/12

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1n-0+deb10u2
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1n-0+deb10u2
```

162549 - Debian DSA-5169-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5169 advisory.

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/security/2022/dsa-5169
https://security-tracker.debian.org/tracker/CVE-2022-2068
https://packages.debian.org/source/buster/openssl
https://packages.debian.org/source/bullseye/openssl

Solution

Upgrade the openssl packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u3.

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

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

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

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

References

CVE CVE-2022-2068

Plugin Information

Published: 2022/06/27, Modified: 2023/10/19

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1n-0+deb10u3
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1n-0+deb10u3
```

201450 - Debian Linux SEoL (10.x) -

Synopsis

An unsupported version of Debian Linux is installed on the remote host.

Description

According to its version, Debian Linux is 10.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

https://www.debian.org/News/2022/20220910

Solution

Upgrade to a version of Debian Linux that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2024/07/03, Modified: 2025/03/26

Plugin Output

tcp/0

```
OS : Debian GNU/Linux 10 (buster)
Security End of Life : September 10, 2022
Time since Security End of Life (Est.) : >= 2 years
```

164946 - Debian dla-3103 : lib32z1 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3103 advisory.

- ---------- Debian LTS Advisory DLA-3103-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 12, 2022 https://wiki.debian.org/LTS
- ----------

Package : zlib Version : 1:1.2.11.dfsg-1+deb10u2 CVE ID : CVE-2022-37434 Debian Bug : 1016710

Evgeny Legerov reported a heap-based buffer overflow vulnerability in the inflate operation in zlib, which could result in denial of service or potentially the execution of arbitrary code if specially crafted input is processed.

For Debian 10 buster, this problem has been fixed in version 1:1.2.11.dfsg-1+deb10u2.

We recommend that you upgrade your zlib packages.

For the detailed security status of zlib please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/zlib

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/zlib
https://security-tracker.debian.org/tracker/CVE-2022-37434
https://packages.debian.org/source/buster/zlib

Solution

Upgrade the lib32z1 packages.

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

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

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

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

References

CVE CVE-2022-37434

Plugin Information

Published: 2022/09/12, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : zlib1g_1:1.2.11.dfsg-1
Should be : zlib1g_1:1.2.11.dfsg-1+deb10u2
```

164992 - Debian dla-3107 : lemon - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3107 advisory.

- ---------- Debian LTS Advisory DLA-3107-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb September 13, 2022 https://wiki.debian.org/LTS
- ----------

Package : sqlite3 Version : 3.27.2-3+deb10u2 CVE IDs : CVE-2020-35525 CVE-2020-35527 CVE-2021-20223

It was discovered that there were three issues in SQLite:

* CVE-2020-35525: Prevent a potential null pointer deference issue in INTERSEC query processing.

* CVE-2020-35527: Prevent an out-of-bounds access issue that could be exploited via ALTER TABLE in views that have a nested FROM clauses.

* CVE-2021-20223: Prevent an issue with the unicode61 tokenizer related to Unicode control characters (class Cc) and embedded NUL characters being misinterpreted as tokens.

For Debian 10 buster, these problems have been fixed in version 3.27.2-3+deb10u2.

We recommend that you upgrade your sqlite3 packages.

For the detailed security status of sqlite3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/sqlite3

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/CVE-2020-35525
https://security-tracker.debian.org/tracker/CVE-2020-35527
https://security-tracker.debian.org/tracker/CVE-2021-20223
https://security-tracker.debian.org/tracker/source-package/sqlite3
https://packages.debian.org/source/buster/sqlite3

Solution

Upgrade the lemon packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-35525
CVE	CVE-2020-35527
CVE	CVE-2021-20223

Plugin Information

Published: 2022/09/13, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libsqlite3-0_3.27.2-3+deb10u1
Should be : libsqlite3-0_3.27.2-3+deb10u2
```

166779 - Debian dla-3175 : idle-python3.7 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3175 advisory.

---------- Debian LTS Advisory DLA-3175-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Stefano Rivera November 01, 2022 https://wiki.debian.org/LTS

Package : python3.7 Version : 3.7.3-2+deb10u4 CVE ID : CVE-2022-37454

Nicky Mouha discovered a buffer overflow in '_sha3', the SHA-3 hashing function module used by 'hashlib' in Python 3.7.

While the attacks require a large volume of data, they could potentially result in remote code execution.

For Debian 10 buster, this problem has been fixed in version 3.7.3-2+deb10u4.

We recommend that you upgrade your python3.7 packages.

For the detailed security status of python3.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python3.7
https://security-tracker.debian.org/tracker/CVE-2022-37454
https://packages.debian.org/source/buster/python3.7

Solution

Upgrade the idle-python3.7 packages.

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

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

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

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

References

CVE CVE-2022-37454

Plugin Information

Published: 2022/11/01, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython3.7-minimal_3.7.3-2+deb10u2
Should be : libpython3.7-minimal_3.7.3-2+deb10u4
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u2
Should be : libpython3.7-stdlib_3.7.3-2+deb10u4
Remote package installed : python3.7_3.7.3-2+deb10u2
Should be : python3.7_3.7.3-2+deb10u4
Remote package installed : python3.7-minimal_3.7.3-2+deb10u2
Should be : python3.7-minimal_3.7.3-2+deb10u4
```

170680 - Debian dla-3282 : git - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3282 advisory.

- ---------- Debian LTS Advisory DLA-3282-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler January 26, 2023 https://wiki.debian.org/LTS
- ----------

Package : git Version : 1:2.20.1-2+deb10u7 CVE ID : CVE-2022-23521 CVE-2022-41903 Debian Bug : 1029114

Two vulnerabilities were discovered in Git, a distributed revision control system. An attacker may trigger code execution in specific situations.

CVE-2022-23521

gitattributes are a mechanism to allow defining attributes for paths. These attributes can be defined by adding a `.gitattributes` file to the repository, which contains a set of file patterns and the attributes that should be set for paths matching this pattern. When parsing gitattributes, multiple integer overflows can occur when there is a huge number of path patterns, a huge number of attributes for a single pattern, or when the declared attribute names are huge. These overflows can be triggered via a crafted `.gitattributes` file that may be part of the commit history. Git silently splits lines longer than 2KB when parsing gitattributes from a file, but not when parsing them from the index. Consequentially, the failure mode depends on whether the file exists in the working tree, the index or both. This integer overflow can result in arbitrary heap reads and writes, which may result in remote code execution.

CVE-2022-41903

`git log` can display commits in an arbitrary format using its `--format` specifiers. This functionality is also exposed to `git archive` via the `export-subst` gitattribute. When processing the padding operators, there is a integer overflow in `pretty.c::format_and_pad_commit()` where a `size_t` is stored improperly as an `int`, and then added as an offset to a `memcpy()`. This overflow can be triggered directly by a user running a command which invokes the commit formatting machinery (e.g., `git log --format=...`). It may also be triggered indirectly through git archive via the export-subst mechanism, which expands format specifiers inside of files within the repository during a git archive. This integer overflow can result in arbitrary heap writes, which may result in arbitrary code execution.

For Debian 10 buster, these problems have been fixed in version 1:2.20.1-2+deb10u7.

We recommend that you upgrade your git packages.

For the detailed security status of git please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/git

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/git
https://security-tracker.debian.org/tracker/CVE-2022-23521
https://security-tracker.debian.org/tracker/CVE-2022-41903
https://packages.debian.org/source/buster/git

Solution

Upgrade the git packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-23521
CVE	CVE-2022-41903

Plugin Information

Published: 2023/01/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : git_1:2.20.1-2+deb10u3
Should be : git_1:2.20.1-2+deb10u7
Remote package installed : git-man_1:2.20.1-2+deb10u3
Should be : git-man_1:2.20.1-2+deb10u7
```

174685 - Debian dla-3398 : curl - security update

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3398 advisory.

---------- Debian LTS Advisory DLA-3398-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany April 21, 2023 https://wiki.debian.org/LTS

Package : curl Version : 7.64.0-4+deb10u6 CVE ID : CVE-2023-27533 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538

Several security vulnerabilities have been found in cURL, an easy-to-use client-side URL transfer library.

CVE-2023-27533

A vulnerability in input validation exists in curl during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and telnet options during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent.
This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system.

CVE-2023-27535

An authentication bypass vulnerability exists in libcurl in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information.

CVE-2023-27536

An authentication bypass vulnerability exists in libcurl in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed.

CVE-2023-27538

An authentication bypass vulnerability exists in libcurl where it reuses a previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match easily, potentially leading to the reuse of an inappropriate connection.

For Debian 10 buster, these problems have been fixed in version 7.64.0-4+deb10u6.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2023-27533
https://security-tracker.debian.org/tracker/CVE-2023-27535
https://security-tracker.debian.org/tracker/CVE-2023-27536
https://security-tracker.debian.org/tracker/CVE-2023-27538
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

STIG Severity

I

References

CVE	CVE-2023-27533
CVE	CVE-2023-27535
CVE	CVE-2023-27536
CVE	CVE-2023-27538
XREF	IAVA:2023-A-0153-S

Plugin Information

Published: 2023/04/25, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u6
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u6
```

174709 - Debian dla-3401 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3401 advisory.

- ---------- Debian LTS Advisory DLA-3401-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris April 24, 2023 https://wiki.debian.org/LTS
- ----------

Package : apache2 Version : 2.4.38-3+deb10u10 CVE ID : CVE-2023-25690 CVE-2023-27522 Debian Bug : 1032476

Several vulnerabilities have been discovered in apache2, a webserver that may be used as front-end proxy for other applications.
These vulnerabilities may lead to HTTP request smuggling, and thus to front-end security controls being bypassed.

Unfortunately, fixing these security vulnerabilities may require changes to configuration files. Some out-of-specification RewriteRule directives that were previously silently accepted, are now rejected with error AH10409. For instance, some RewriteRules that included a back-reference and the flags [L,NC] will need to be written with extra escaping flags such as [B= ?,BNP,QSA].

CVE-2023-25690

Some mod_proxy configurations allow an HTTP request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

CVE-2023-27522

HTTP Response Smuggling in mod_proxy_uwsgi

For Debian 10 buster, these problems have been fixed in version 2.4.38-3+deb10u10.

We recommend that you upgrade your apache2 packages.

For the detailed security status of apache2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/apache2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://security-tracker.debian.org/tracker/CVE-2023-25690
https://security-tracker.debian.org/tracker/CVE-2023-27522
https://packages.debian.org/source/buster/apache2

Solution

Upgrade the apache2 packages.

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

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

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

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

STIG Severity

I

References

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XREF	IAVA:2023-A-0124-S

Plugin Information

Published: 2023/04/25, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.38-3+deb10u10
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.38-3+deb10u10
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.38-3+deb10u10
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.38-3+deb10u10
```

179924 - Debian dla-3532 : openssh-client - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3532 advisory.

- ---------- Debian LTS Advisory DLA-3532-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Utkarsh Gupta August 17, 2023 https://wiki.debian.org/LTS
- ----------

Package : openssh Version : 1:7.9p1-10+deb10u3 CVE ID : CVE-2023-38408 Debian Bug : 1042460

It was discovered that OpenSSH incorrectly handled loading certain PKCS#11 providers. If a user forwarded their ssh-agent to an untrusted system, a remote attacker could possibly use this issue to load arbitrary libraries from the users system and execute arbitrary code.

In addition to the above security issue, this update also fixed another bug - bad interaction between the ssh_config ConnectTimeout and ConnectionAttempts directives - connection attempts after the first attempt were ignoring the requested timeout. More details about this can be found at https://bugzilla.mindrot.org/show_bug.cgi?id=2918.

For Debian 10 buster, this problem has been fixed in version 1:7.9p1-10+deb10u3.

We recommend that you upgrade your openssh packages.

For the detailed security status of openssh please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssh

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssh
https://security-tracker.debian.org/tracker/CVE-2023-38408
https://packages.debian.org/source/buster/openssh

Solution

Upgrade the openssh-client packages.

Risk Factor

Critical

CVSS v4.0 Base Score

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

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

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

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

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

STIG Severity

I

References

CVE	CVE-2023-38408
XREF	IAVA:2023-A-0377-S

Plugin Information

Published: 2023/08/17, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : openssh-client_1:7.9p1-10+deb10u2
Should be : openssh-client_1:7.9p1-10+deb10u3
Remote package installed : openssh-server_1:7.9p1-10+deb10u2
Should be : openssh-server_1:7.9p1-10+deb10u3
Remote package installed : openssh-sftp-server_1:7.9p1-10+deb10u2
Should be : openssh-sftp-server_1:7.9p1-10+deb10u3
```

182942 - Debian dla-3614 : idle-python3.7 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3614 advisory.

---------- Debian LTS Advisory DLA-3614-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton October 11, 2023 https://wiki.debian.org/LTS

Package : python3.7 Version : 3.7.3-2+deb10u6 CVE ID : CVE-2022-48560 CVE-2022-48564 CVE-2022-48565 CVE-2022-48566 CVE-2023-40217

Several vulnerabilities were discovered in Python 3.7.

CVE-2022-48560

A use-after-free problem was found in the heappushpop function in the heapq module.

CVE-2022-48564

A potential denial-of-service vulnerability was discovered in the read_ints function used when processing certain malformed Apple Property List files in binary format.

CVE-2022-48565

An XML External Entity (XXE) issue was discovered. In order to avoid possible vulnerabilities, the plistlib module no longer accepts entity declarations in XML plist files.

CVE-2022-48566

Possible constant-time-defeating compiler optimisations were discovered in the accumulator variable in hmac.compare_digest.

CVE-2023-40217

It was discovered that it might be possible to bypass some of the protections implemented by the TLS handshake in the ssl.SSLSocket class. For example, unauthenticated data might be read by a program expecting data authenticated by client certificates.

For Debian 10 buster, these problems have been fixed in version 3.7.3-2+deb10u6.

We recommend that you upgrade your python3.7 packages.

For the detailed security status of python3.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python3.7
https://security-tracker.debian.org/tracker/CVE-2022-48560
https://security-tracker.debian.org/tracker/CVE-2022-48564
https://security-tracker.debian.org/tracker/CVE-2022-48565
https://security-tracker.debian.org/tracker/CVE-2022-48566
https://security-tracker.debian.org/tracker/CVE-2023-40217
https://packages.debian.org/source/buster/python3.7

Solution

Upgrade the idle-python3.7 packages.

Risk Factor

Critical

CVSS v4.0 Base Score

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

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

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

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

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

References

CVE	CVE-2022-48560
CVE	CVE-2022-48564
CVE	CVE-2022-48565
CVE	CVE-2022-48566
CVE	CVE-2023-40217

Plugin Information

Published: 2023/10/11, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython3.7-minimal_3.7.3-2+deb10u2
Should be : libpython3.7-minimal_3.7.3-2+deb10u6
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u2
Should be : libpython3.7-stdlib_3.7.3-2+deb10u6
Remote package installed : python3.7_3.7.3-2+deb10u2
Should be : python3.7_3.7.3-2+deb10u6
Remote package installed : python3.7-minimal_3.7.3-2+deb10u2
Should be : python3.7-minimal_3.7.3-2+deb10u6
```

146389 - Debian DSA-4850-1 : libzstd - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

It was discovered that zstd, a compression utility, temporarily exposed a world-readable version of its input even if the original file had restrictive permissions.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=981404
https://security-tracker.debian.org/tracker/source-package/libzstd
https://packages.debian.org/source/buster/libzstd
https://www.debian.org/security/2021/dsa-4850

Solution

Upgrade the libzstd packages.

For the stable distribution (buster), this problem has been fixed in version 1.3.8+dfsg-3+deb10u1.

Risk Factor

High

References

XREF	DSA:4850

Plugin Information

Published: 2021/02/11, Modified: 2021/02/11

Plugin Output

tcp/0

```
Remote package installed : libzstd1_1.3.8+dfsg-3
Should be : libzstd1_1.3.8+dfsg-3+deb10u1
```

146787 - Debian DSA-4859-1 : libzstd - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

It was discovered that zstd, a compression utility, was vulnerable to a race condition: it temporarily exposed, during a very short timeframe, a world-readable version of its input even if the original file had restrictive permissions.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=982519
https://security-tracker.debian.org/tracker/source-package/libzstd
https://packages.debian.org/source/buster/libzstd
https://www.debian.org/security/2021/dsa-4859

Solution

Upgrade the libzstd packages.

For the stable distribution (buster), this problem has been fixed in version 1.3.8+dfsg-3+deb10u2.

Risk Factor

High

References

XREF DSA:4859

Plugin Information

Published: 2021/02/23, Modified: 2021/02/23

Plugin Output

tcp/0

```
Remote package installed : libzstd1_1.3.8+dfsg-3
Should be : libzstd1_1.3.8+dfsg-3+deb10u2
```

149855 - Debian DSA-4919-1 : lz4 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Jasper Lievisse Adriaanse reported an integer overflow flaw in lz4, a fast LZ compression algorithm library, resulting in memory corruption.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=987856
https://security-tracker.debian.org/tracker/source-package/lz4
https://packages.debian.org/source/buster/lz4
https://www.debian.org/security/2021/dsa-4919

Solution

Upgrade the lz4 packages.

For the stable distribution (buster), this problem has been fixed in version 1.8.3-1+deb10u1.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3520
XREF	DSA:4919

Plugin Information

Published: 2021/05/24, Modified: 2021/06/15

Plugin Output

tcp/0

```
Remote package installed : liblz4-1_1.8.3-1
Should be : liblz4-1_1.8.3-1+deb10u1
```

149897 - Debian DSA-4920-1 : libx11 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Roman Fiedler reported that missing length validation in various functions provided by libx11, the X11 client-side library, allow to inject X11 protocol commands on X clients, leading to authentication bypass, denial of service or potentially the execution of arbitrary code.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=988737
https://security-tracker.debian.org/tracker/source-package/libx11
https://packages.debian.org/source/buster/libx11
https://www.debian.org/security/2021/dsa-4920

Solution

Upgrade the libx11 packages.

For the stable distribution (buster), this problem has been fixed in version 2:1.6.7-1+deb10u2.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-31535
XREF	DSA:4920

Plugin Information

Published: 2021/05/25, Modified: 2021/06/14

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.7-1+deb10u1
Should be : libx11-6_2:1.6.7-1+deb10u2
Remote package installed : libx11-data_2:1.6.7-1+deb10u1
Should be : libx11-data_2:1.6.7-1+deb10u2
```

151485 - Debian DSA-4937-1 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-4937 advisory.

- Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow (CVE-2020-35452)

- Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service (CVE-2021-26690)

- In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow (CVE-2021-26691)

- Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'
(CVE-2021-30641)

- Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server. This issue affected mod_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released. (CVE-2021-31618)

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/security/2021/dsa-4937
https://security-tracker.debian.org/tracker/CVE-2020-35452
https://security-tracker.debian.org/tracker/CVE-2021-26690
https://security-tracker.debian.org/tracker/CVE-2021-26691
https://security-tracker.debian.org/tracker/CVE-2021-30641
https://security-tracker.debian.org/tracker/CVE-2021-31618
https://packages.debian.org/source/buster/apache2

Solution

Upgrade the apache2 packages.

For the stable distribution (buster), these problems have been fixed in version 2.4.38-3+deb10u5.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-35452
CVE	CVE-2021-26690
CVE	CVE-2021-26691
CVE	CVE-2021-30641
CVE	CVE-2021-31618
XREF	IAVA:2021-A-0259-S

Plugin Information

Published: 2021/07/09, Modified: 2021/09/24

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.38-3+deb10u5
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.38-3+deb10u5
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.38-3+deb10u5
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.38-3+deb10u5
```

152783 - Debian DSA-4963-1 : openssl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-4963 advisory.

Multiple vulnerabilities have been discovered in OpenSSL, a Secure Sockets Layer toolkit. CVE-2021-3711 John Ouyang reported a buffer overflow vulnerability in the SM2 decryption. An attacker able to present SM2 content for decryption to an application can take advantage of this flaw to change application behaviour or cause the application to crash (denial of service). CVE-2021-3712 Ingo Schwarze reported a buffer overrun flaw when processing ASN.1 strings in the X509_aux_print() function, which can result in denial of service. Additional details can be found in the upstream advisory: https://www.openssl.org/news/secadv/20210824.txt For the oldstable distribution (buster), these problems have been fixed in version 1.1.1d-0+deb10u7. For the stable distribution (bullseye), these problems have been fixed in version 1.1.1k-1+deb11u1. We recommend that you upgrade your openssl packages. For the detailed security status of openssl please refer to its security tracker page at: https://security- tracker.debian.org/tracker/openssl

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/security/2021/dsa-4963
https://security-tracker.debian.org/tracker/CVE-2021-3711
https://security-tracker.debian.org/tracker/CVE-2021-3712
https://packages.debian.org/source/buster/openssl
https://packages.debian.org/source/bullseye/openssl

Solution

Upgrade the openssl packages.

For the stable distribution (bullseye), these problems have been fixed in version 1.1.1k-1+deb11u1.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3711
CVE	CVE-2021-3712
XREF	IAVA:2021-A-0395-S

Plugin Information

Published: 2021/08/24, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1d-0+deb10u7
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1d-0+deb10u7
```

153970 - Debian DSA-4982-1 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-4982 advisory.

Several vulnerabilities have been found in the Apache HTTP server, which could result in denial of service. In addition a vulnerability was discovered in mod_proxy with which an attacker could trick the server to forward requests to arbitrary origin servers. For the oldstable distribution (buster), these problems have been fixed in version 2.4.38-3+deb10u6. For the stable distribution (bullseye), these problems have been fixed in version 2.4.51-1~deb11u1. We recommend that you upgrade your apache2 packages.
For the detailed security status of apache2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/apache2

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/security/2021/dsa-4982
https://security-tracker.debian.org/tracker/CVE-2021-34798
https://security-tracker.debian.org/tracker/CVE-2021-36160
https://security-tracker.debian.org/tracker/CVE-2021-39275
https://security-tracker.debian.org/tracker/CVE-2021-40438
https://packages.debian.org/source/buster/apache2
https://packages.debian.org/source/bullseye/apache2

Solution

Upgrade the apache2 packages.

For the stable distribution (bullseye), these problems have been fixed in version 2.4.51-1~deb11u1.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-36160
CVE	CVE-2021-39275
CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/10/10, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.38-3+deb10u6
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.38-3+deb10u6
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.38-3+deb10u6
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.38-3+deb10u6
```

155769 - Debian DSA-5016-1 : nss - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5016 advisory.

Tavis Ormandy discovered that nss, the Mozilla Network Security Service library, is prone to a heap overflow flaw when verifying DSA or RSA-PPS signatures, which could result in denial of service or potentially the execution of arbitrary code. For the oldstable distribution (buster), this problem has been fixed in version 2:3.42.1-1+deb10u4. For the stable distribution (bullseye), this problem has been fixed in version 2:3.61-1+deb11u1. We recommend that you upgrade your nss packages. For the detailed security status of nss please refer to its security tracker page at: https://security- tracker.debian.org/tracker/nss

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nss
https://www.debian.org/security/2021/dsa-5016
https://security-tracker.debian.org/tracker/CVE-2021-43527
https://packages.debian.org/source/buster/nss
https://packages.debian.org/source/bullseye/nss

Solution

Upgrade the nss packages.

For the stable distribution (bullseye), this problem has been fixed in version 2

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-43527

Plugin Information

Published: 2021/12/02, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libnss3_2:3.42.1-1+deb10u3
Should be : libnss3_2:3.42.1-1+deb10u4
```

156466 - Debian DSA-5035-1 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5035 advisory.

- A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included). (CVE-2021-44224)

- A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier. (CVE-2021-44790)

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/security/2022/dsa-5035
https://security-tracker.debian.org/tracker/CVE-2021-44224
https://security-tracker.debian.org/tracker/CVE-2021-44790
https://packages.debian.org/source/buster/apache2
https://packages.debian.org/source/bullseye/apache2

Solution

Upgrade the apache2 packages.

For the stable distribution (bullseye), these problems have been fixed in version 2.4.52-1~deb11u2.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44224
CVE	CVE-2021-44790
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2022/01/05, Modified: 2023/11/21

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.38-3+deb10u7
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.38-3+deb10u7
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.38-3+deb10u7
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.38-3+deb10u7
```

157249 - Debian DSA-5062-1 : nss - security update

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5062 advisory.

- After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. (CVE-2022-22747)

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

See Also

https://security-tracker.debian.org/tracker/source-package/nss
https://www.debian.org/security/2022/dsa-5062
https://security-tracker.debian.org/tracker/CVE-2022-22747
https://packages.debian.org/source/buster/nss
https://packages.debian.org/source/bullseye/nss

Solution

Upgrade the nss packages.

For the stable distribution (bullseye), this problem has been fixed in version 2

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-22747
XREF	IAVA:2022-A-0017-S

Plugin Information

Published: 2022/01/31, Modified: 2023/03/21

Plugin Output

tcp/0

```
Remote package installed : libnss3_2:3.42.1-1+deb10u3
Should be : libnss3_2:3.42.1-1+deb10u5
```

158031 - Debian DSA-5073-1 : expat - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5073 advisory.

- In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).
(CVE-2021-45960)

- In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize. (CVE-2021-46143)

- addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22822)

- build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22823)

- defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
(CVE-2022-22824)

- lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22825)

- nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
(CVE-2022-22826)

- storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22827)

- Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES. (CVE-2022-23852)

- Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function. (CVE-2022-23990)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1002994
https://security-tracker.debian.org/tracker/source-package/expat
https://www.debian.org/security/2022/dsa-5073
https://security-tracker.debian.org/tracker/CVE-2021-45960
https://security-tracker.debian.org/tracker/CVE-2021-46143

https://security-tracker.debian.org/tracker/CVE-2022-22822
https://security-tracker.debian.org/tracker/CVE-2022-22823
https://security-tracker.debian.org/tracker/CVE-2022-22824
https://security-tracker.debian.org/tracker/CVE-2022-22825
https://security-tracker.debian.org/tracker/CVE-2022-22826
https://security-tracker.debian.org/tracker/CVE-2022-22827
https://security-tracker.debian.org/tracker/CVE-2022-23852
https://security-tracker.debian.org/tracker/CVE-2022-23990
https://packages.debian.org/source/buster/expat
https://packages.debian.org/source/bullseye/expat

Solution

Upgrade the expat packages.

For the stable distribution (bullseye), these problems have been fixed in version 2.2.10-2+deb11u1.

For the oldstable distribution (buster), these problems have been fixed in version 2.2.6-2+deb10u2.

Risk Factor

High

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

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

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)

References

CVE	CVE-2021-45960
CVE	CVE-2021-46143
CVE	CVE-2022-22822
CVE	CVE-2022-22823
CVE	CVE-2022-22824
CVE	CVE-2022-22825
CVE	CVE-2022-22826
CVE	CVE-2022-22827
CVE	CVE-2022-23852
CVE	CVE-2022-23990

Plugin Information

Published: 2022/02/13, Modified: 2023/11/09

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.6-2+deb10u1
Should be : libexpat1_2.2.6-2+deb10u2
```

158270 - Debian DSA-5085-1 : expat - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5085 advisory.

- xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context. (CVE-2022-25235)

- xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs. (CVE-2022-25236)

- In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element. (CVE-2022-25313)

- In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString. (CVE-2022-25314)

- In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames. (CVE-2022-25315)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1005894
https://security-tracker.debian.org/tracker/source-package/expat
https://www.debian.org/security/2022/dsa-5085
https://security-tracker.debian.org/tracker/CVE-2022-25235
https://security-tracker.debian.org/tracker/CVE-2022-25236
https://security-tracker.debian.org/tracker/CVE-2022-25313
https://security-tracker.debian.org/tracker/CVE-2022-25314
https://security-tracker.debian.org/tracker/CVE-2022-25315
https://packages.debian.org/source/buster/expat
https://packages.debian.org/source/bullseye/expat

Solution

Upgrade the expat packages.

For the stable distribution (bullseye), these problems have been fixed in version 2.2.10-2+deb11u2.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-25235
CVE	CVE-2022-25236
CVE	CVE-2022-25313
CVE	CVE-2022-25314
CVE	CVE-2022-25315

Plugin Information

Published: 2022/02/23, Modified: 2023/11/07

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.6-2+deb10u1
Should be : libexpat1_2.2.6-2+deb10u3
```

158761 - Debian DSA-5096-1 : linux - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5096 advisory.

- An issue was discovered in the Linux kernel before 5.7.3, related to mm/gup.c and mm/huge_memory.c. The get_user_pages (aka gup) implementation, when

used for a copy-on-write page, does not properly consider the semantics of read operations and therefore can grant unintended write access, aka CID-17839856fd58.
(CVE-2020-29374)

- An issue was discovered in the FUSE filesystem implementation in the Linux kernel before 5.10.6, aka CID-5d069dbe8aaf. fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. NOTE: the original fix for this vulnerability was incomplete, and its incompleteness is tracked as CVE-2021-28950. (CVE-2020-36322)

- A flaw was found in the Linux kernel. A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP.
(CVE-2021-20317)

- A race condition accessing file object in the Linux kernel OverlayFS subsystem was found in the way users do rename in specific way with OverlayFS. A local user could use this flaw to crash the system.
(CVE-2021-20321)

- A flaw in the processing of received ICMP errors (ICMP fragment needed and ICMP redirect) in the Linux kernel functionality was found to allow the ability to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass the source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. (CVE-2021-20322)

- A double free bug in packet_set_ring() in net/packet/af_packet.c can be exploited by a local user through crafted syscalls to escalate privileges or deny service. We recommend upgrading kernel past the effected versions or rebuilding past ec6af094ea28f0f2dda1a6a33b14cd57e36a9755 (CVE-2021-22600)

- Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as driver domains. Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713 (CVE-2021-28711, CVE-2021-28712, CVE-2021-28713)

- Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default).
Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time.
(CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714) (CVE-2021-28714, CVE-2021-28715)

- An issue was discovered in fs/fuse/fuse_i.h in the Linux kernel before 5.11.8. A stall on CPU can occur because a retry loop continually finds the same bad inode, aka CID-775c5033a0d1. (CVE-2021-28950)

- A flaw use-after-free in function sco_sock_sendmsg() of the Linux kernel HCI subsystem was found in the way user calls ioct UFFDIO_REGISTER or other way triggers race condition of the call sco_conn_del() together with the call sco_sock_sendmsg() with the expected controllable faulting memory page. A privileged local user could use this flaw to crash the system or escalate their privileges on the system.
(CVE-2021-3640)

- A memory leak flaw was found in the Linux kernel in the ccp_run_aes_gcm_cmd() function in drivers/crypto/ccp/ccp-ops.c, which allows attackers to cause a denial of service (memory consumption).
This vulnerability is similar with the older CVE-2019-18808. (CVE-2021-3744)

- A use-after-free flaw was found in the Linux kernel's Bluetooth subsystem in the way user calls connect to the socket and disconnect simultaneously due to a race condition. This flaw allows a user to crash the system or escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. (CVE-2021-3752)

- A flaw was found in the Linux kernel. A use-after-free vulnerability in the NFC stack can lead to a threat to confidentiality, integrity, and system availability. (CVE-2021-3760)

- A flaw was found in the Linux SCTP stack. A blind attacker may be able to kill an existing SCTP association through invalid chunks if the attacker knows the IP-addresses and port numbers being used and the attacker can send packets with spoofed IP addresses. (CVE-2021-3772)

- arch/mips/net/bpf_jit.c in the Linux kernel before 5.4.10 can generate undesirable machine code when transforming unprivileged cBPF programs, allowing execution of arbitrary code within the kernel context.
This occurs because conditional branches can exceed the 128 KB limit of the MIPS architecture.
(CVE-2021-38300)

- A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data. (CVE-2021-4002)

- A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system.
This flaw affects Linux kernel versions prior to 5.16-rc4. (CVE-2021-4083)

- prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel before 5.14.12 allows unprivileged users to trigger an eBPF multiplication integer

overflow with a resultant out-of-bounds write. (CVE-2021-41864)

- The firewire subsystem in the Linux kernel through 5.14.13 has a buffer overflow related to drivers/media/firewire/firedtv-avc.c and drivers/media/firewire/firedtv-ci.c, because avc_ca_pmt mishandles bounds checking. (CVE-2021-42739)

- An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c. (CVE-2021-43389)

- In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value. (CVE-2021-43975)

- In the Linux kernel through 5.15.2, mwifiex_usb_recv in drivers/net/wireless/marvell/mwifiex/usb.c allows an attacker (who can connect a crafted USB device) to cause a denial of service (skb_over_panic).
(CVE-2021-43976)

- A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11.
This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a shared memory object. (CVE-2021-44733)

- pep_sock_accept in net/phonet/pep.c in the Linux kernel through 5.15.8 has a refcount leak.
(CVE-2021-45095)

- In __f2fs_setxattr in fs/f2fs/xattr.c in the Linux kernel through 5.15.11, there is an out-of-bounds memory access when an inode has an invalid last xattr entry.
(CVE-2021-45469)

- An issue was discovered in the Linux kernel before 5.15.11. There is a memory leak in the __rds_conn_create() function in net/rds/connection.c in a certain combination of circumstances.
(CVE-2021-45480)

- A use-after-free vulnerability was found in rtsx_usb_ms_drv_remove in drivers/memstick/host/rtsx_usb_ms.c in memstick in the Linux kernel. In this flaw, a local attacker with a user privilege may impact system Confidentiality. This flaw affects kernel versions prior to 5.14 rc1. (CVE-2022-0487)

- A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
(CVE-2022-0492)

- A flaw null pointer dereference in the Linux kernel UDF file system functionality was found in the way user triggers udf_file_write_iter function for the malicious UDF image. A local user could use this flaw to crash the system. Actual from Linux kernel 4.2-rc1 till 5.17-rc2. (CVE-2022-0617)

- An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor. (CVE-2022-24448)

- An issue was discovered in the Linux kernel before 5.16.5. There is a memory leak in yam_siocdevprivate in drivers/net/hamradio/yam.c. (CVE-2022-24959)

- An issue was discovered in drivers/usb/gadget/composite.c in the Linux kernel before 5.16.10. The USB Gadget subsystem lacks certain validation of interface OS descriptor requests (ones with a large array index and ones associated with NULL function pointer retrieval). Memory corruption might occur.
(CVE-2022-25258)

- An issue was discovered in drivers/usb/gadget/function/rndis.c in the Linux kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory. (CVE-2022-25375)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=988044
https://security-tracker.debian.org/tracker/source-package/linux
https://www.debian.org/security/2022/dsa-5096
https://security-tracker.debian.org/tracker/CVE-2020-29374
https://security-tracker.debian.org/tracker/CVE-2020-36322
https://security-tracker.debian.org/tracker/CVE-2021-20317
https://security-tracker.debian.org/tracker/CVE-2021-20321
https://security-tracker.debian.org/tracker/CVE-2021-20322
https://security-tracker.debian.org/tracker/CVE-2021-22600
https://security-tracker.debian.org/tracker/CVE-2021-28711
https://security-tracker.debian.org/tracker/CVE-2021-28712
https://security-tracker.debian.org/tracker/CVE-2021-28713
https://security-tracker.debian.org/tracker/CVE-2021-28714
https://security-tracker.debian.org/tracker/CVE-2021-28715
https://security-tracker.debian.org/tracker/CVE-2021-28950
https://security-tracker.debian.org/tracker/CVE-2021-3640
https://security-tracker.debian.org/tracker/CVE-2021-3744
https://security-tracker.debian.org/tracker/CVE-2021-3752
https://security-tracker.debian.org/tracker/CVE-2021-3760
https://security-tracker.debian.org/tracker/CVE-2021-3764
https://security-tracker.debian.org/tracker/CVE-2021-3772

https://security-tracker.debian.org/tracker/CVE-2021-38300
https://security-tracker.debian.org/tracker/CVE-2021-39685
https://security-tracker.debian.org/tracker/CVE-2021-39686
https://security-tracker.debian.org/tracker/CVE-2021-39698
https://security-tracker.debian.org/tracker/CVE-2021-39713
https://security-tracker.debian.org/tracker/CVE-2021-4002
https://security-tracker.debian.org/tracker/CVE-2021-4083
https://security-tracker.debian.org/tracker/CVE-2021-4135
https://security-tracker.debian.org/tracker/CVE-2021-4155
https://security-tracker.debian.org/tracker/CVE-2021-41864
https://security-tracker.debian.org/tracker/CVE-2021-4202
https://security-tracker.debian.org/tracker/CVE-2021-4203
https://security-tracker.debian.org/tracker/CVE-2021-42739
https://security-tracker.debian.org/tracker/CVE-2021-43389
https://security-tracker.debian.org/tracker/CVE-2021-43975
https://security-tracker.debian.org/tracker/CVE-2021-43976
https://security-tracker.debian.org/tracker/CVE-2021-44733
https://security-tracker.debian.org/tracker/CVE-2021-45095
https://security-tracker.debian.org/tracker/CVE-2021-45469
https://security-tracker.debian.org/tracker/CVE-2021-45480
https://security-tracker.debian.org/tracker/CVE-2022-0001
https://security-tracker.debian.org/tracker/CVE-2022-0002
https://security-tracker.debian.org/tracker/CVE-2022-0322
https://security-tracker.debian.org/tracker/CVE-2022-0330
https://security-tracker.debian.org/tracker/CVE-2022-0435
https://security-tracker.debian.org/tracker/CVE-2022-0487
https://security-tracker.debian.org/tracker/CVE-2022-0492
https://security-tracker.debian.org/tracker/CVE-2022-0617
https://security-tracker.debian.org/tracker/CVE-2022-0644
https://security-tracker.debian.org/tracker/CVE-2022-22942
https://security-tracker.debian.org/tracker/CVE-2022-24448
https://security-tracker.debian.org/tracker/CVE-2022-24959
https://security-tracker.debian.org/tracker/CVE-2022-25258
https://security-tracker.debian.org/tracker/CVE-2022-25375
https://packages.debian.org/source/buster/linux

Solution

Upgrade the linux packages.

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

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

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

7.8 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2020-29374
CVE	CVE-2020-36322
CVE	CVE-2021-3640
CVE	CVE-2021-3744
CVE	CVE-2021-3752
CVE	CVE-2021-3760
CVE	CVE-2021-3764
CVE	CVE-2021-3772
CVE	CVE-2021-4002
CVE	CVE-2021-4083
CVE	CVE-2021-4135
CVE	CVE-2021-4155
CVE	CVE-2021-4202
CVE	CVE-2021-4203
CVE	CVE-2021-20317
CVE	CVE-2021-20321
CVE	CVE-2021-20322
CVE	CVE-2021-22600
CVE	CVE-2021-28711
CVE	CVE-2021-28712

CVE	CVE-2021-28713
CVE	CVE-2021-28714
CVE	CVE-2021-28715
CVE	CVE-2021-28950
CVE	CVE-2021-38300
CVE	CVE-2021-39685
CVE	CVE-2021-39686
CVE	CVE-2021-39698
CVE	CVE-2021-39713
CVE	CVE-2021-41864
CVE	CVE-2021-42739
CVE	CVE-2021-43389
CVE	CVE-2021-43975
CVE	CVE-2021-43976
CVE	CVE-2021-44733
CVE	CVE-2021-45095
CVE	CVE-2021-45469
CVE	CVE-2021-45480
CVE	CVE-2022-0001
CVE	CVE-2022-0002
CVE	CVE-2022-0322
CVE	CVE-2022-0330
CVE	CVE-2022-0435
CVE	CVE-2022-0487
CVE	CVE-2022-0492
CVE	CVE-2022-0617
CVE	CVE-2022-0644
CVE	CVE-2022-22942
CVE	CVE-2022-24448
CVE	CVE-2022-24959
CVE	CVE-2022-25258
CVE	CVE-2022-25375
XREF	CISA-KNOWN-EXPLOITED:2022/05/02

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/03/09, Modified: 2024/03/27

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.19.0-14-amd64_4.19.171-2
Should be : linux-image-4.19.0-<ANY>-amd64_4.19.232-1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

159906 - Debian DSA-5122-1 : gzip - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5122 advisory.

cleemy desu wayo reported that incorrect handling of filenames by zgrep in gzip, the GNU compression utilities, can result in overwrite of arbitrary files or execution of arbitrary code if a file with a specially crafted filename is processed. For the oldstable distribution (buster), this problem has been fixed in version 1.9-3+deb10u1. For the stable distribution (bullseye), this problem has been fixed in version 1.10-4+deb11u1. We recommend that you upgrade your gzip packages. For the detailed security status of gzip please refer to its security tracker page at: https://security-tracker.debian.org/tracker/gzip

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

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1009168
https://security-tracker.debian.org/tracker/source-package/gzip
https://www.debian.org/security/2022/dsa-5122

https://security-tracker.debian.org/tracker/CVE-2022-1271
https://packages.debian.org/source/buster/gzip
https://packages.debian.org/source/bullseye/gzip

Solution

Upgrade the gzip packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.10-4+deb11u1.

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)

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-2022-1271
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/19, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : gzip_1.9-3
Should be : gzip_1.9-3+deb10u1
```

159904 - Debian DSA-5123-1 : xz-utils - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5123 advisory.

- An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system. (CVE-2022-1271)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1009167
https://security-tracker.debian.org/tracker/source-package/xz-utils
https://www.debian.org/security/2022/dsa-5123
https://security-tracker.debian.org/tracker/CVE-2022-1271
https://packages.debian.org/source/buster/xz-utils
https://packages.debian.org/source/bullseye/xz-utils

Solution

Upgrade the xz-utils packages.

For the stable distribution (bullseye), this problem has been fixed in version 5.2.5-2.1~deb11u1.

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)

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-2022-1271
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/19, Modified: 2024/06/07

Plugin Output

tcp/0

```
Remote package installed : liblzma5_5.2.4-1
Should be : liblzma5_5.2.4-1+deb10u1
Remote package installed : xz-utils_5.2.4-1
Should be : xz-utils_5.2.4-1+deb10u1
```

161404 - Debian DSA-5140-1 : openldap - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5140 advisory.

- In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental back-sql backend to slapd, via a SQL statement within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to a lack of proper escaping. (CVE-2022-29155)

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

See Also

https://security-tracker.debian.org/tracker/source-package/openldap
https://www.debian.org/security/2022/dsa-5140
https://security-tracker.debian.org/tracker/CVE-2022-29155
https://packages.debian.org/source/buster/openldap
https://packages.debian.org/source/bullseye/openldap

Solution

Upgrade the openldap packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.4.57+dfsg-3+deb11u1.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-29155

Plugin Information

Published: 2022/05/20, Modified: 2023/10/26

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.47+dfsg-3+deb10u6
Should be : libldap-2.4-2_2.4.47+dfsg-3+deb10u7
Remote package installed : libldap-common_2.4.47+dfsg-3+deb10u6
Should be : libldap-common_2.4.47+dfsg-3+deb10u7
```

161513 - Debian DSA-5147-1 : dpkg - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5147 advisory.

- Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-place extraction can lead to directory traversal situations on specially crafted orig.tar and debian.tar tarballs. (CVE-2022-1664)

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

See Also

https://security-tracker.debian.org/tracker/source-package/dpkg
https://www.debian.org/security/2022/dsa-5147
https://security-tracker.debian.org/tracker/CVE-2022-1664
https://packages.debian.org/source/buster/dpkg
https://packages.debian.org/source/bullseye/dpkg

Solution

Upgrade the dpkg packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.20.10.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-1664

Plugin Information

Published: 2022/05/26, Modified: 2022/06/08

Plugin Output

tcp/0

```
Remote package installed : dpkg_1.19.7
Should be : dpkg_1.19.8
```

164081 - Debian dla-3070 : gnutls-bin - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3070 advisory.

- ---------- Debian LTS Advisory DLA-3070-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort August 11, 2022 https://wiki.debian.org/LTS
- ----------

Package : gnutls28 Version : 3.6.7-4+deb10u9 CVE ID : CVE-2021-4209 CVE-2022-2509

Two issues were found in GnuTLS, a library implementing the TLS and SSL protocols. A remote attacker could take advantage of these flaws to cause an application using the GnuTLS library to crash (denial of service), or potentially, to execute arbitrary code.

For Debian 10 buster, these problems have been fixed in version 3.6.7-4+deb10u9.

We recommend that you upgrade your gnutls28 packages.

For the detailed security status of gnutls28 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/gnutls28

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/gnutls28
https://security-tracker.debian.org/tracker/CVE-2021-4209
https://security-tracker.debian.org/tracker/CVE-2022-2509
https://packages.debian.org/source/buster/gnutls28

Solution

Upgrade the gnutls-bin packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-4209
CVE	CVE-2022-2509

Plugin Information

Published: 2022/08/11, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libgnutls30_3.6.7-4+deb10u6
Should be : libgnutls30_3.6.7-4+deb10u9
```

165217 - Debian dla-3112 : bzip2 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3112 advisory.

- ---------- Debian LTS Advisory DLA-3112-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 16, 2022 https://wiki.debian.org/LTS
- ----------

Package : bzip2 Version : 1.0.6-9.2~deb10u2 Debian Bug : 944557 965309

This update fixes bzdiff when using it with two compressed files. It also includes a fix to support large files on 32 bit systems.

For Debian 10 buster, this problem has been fixed in version 1.0.6-9.2~deb10u2.

We recommend that you upgrade your bzip2 packages.

For the detailed security status of bzip2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/bzip2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/bzip2
https://packages.debian.org/source/buster/bzip2

Solution

Upgrade the bzip2 packages.

Risk Factor

High

Plugin Information

Published: 2022/09/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : bzip2_1.0.6-9.2~deb10u1
Should be : bzip2_1.0.6-9.2~deb10u2
Remote package installed : libbz2-1.0_1.0.6-9.2~deb10u1
Should be : libbz2-1.0_1.0.6-9.2~deb10u2
```

165477 - Debian dla-3119 : expat - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3119 advisory.

- ---------- Debian LTS Advisory DLA-3119-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz September 25, 2022 https://wiki.debian.org/LTS
- ----------

Package : expat Version : 2.2.6-2+deb10u5 CVE ID : CVE-2022-40674

Rhodri James discovered a heap use-after-free vulnerability in the doContent function in Expat, an XML parsing C library, which could result in denial of service or potentially the execution of arbitrary code, if a malformed XML file is processed.

For Debian 10 buster, this problem has been fixed in version 2.2.6-2+deb10u5.

We recommend that you upgrade your expat packages.

For the detailed security status of expat please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/expat

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/expat
https://security-tracker.debian.org/tracker/CVE-2022-40674
https://packages.debian.org/source/buster/expat

Solution

Upgrade the expat packages.

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)

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

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

References

CVE CVE-2022-40674

Plugin Information

Published: 2022/09/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.6-2+deb10u1
Should be : libexpat1_2.2.6-2+deb10u5
```

165642 - Debian dla-3134 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3134 advisory.

- ---------- Debian LTS Advisory DLA-3134-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 03, 2022 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2021a-0+deb10u7

This update includes the changes in tzdata 2022d. Notable changes are:

- - Palestine now switches back to standard time on October 29.
- - Updated leap second list, which was set to expire by the end of December.

For Debian 10 buster, this problem has been fixed in version 2021a-0+deb10u7.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2022/10/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
Should be : tzdata_2021a-0+deb10u7
```

165715 - Debian dla-3138 : bind9 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3138 advisory.

- ---------- Debian LTS Advisory DLA-3138-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 05, 2022 https://wiki.debian.org/LTS
- ----------

Package : bind9 Version : 1:9.11.5.P4+dfsg-5.1+deb10u8 CVE ID : CVE-2022-2795 CVE-2022-38177 CVE-2022-38178

Several vulnerabilities were discovered in BIND, a DNS server implementation.

CVE-2022-2795

Yehuda Afek, Anat Bremler-Barr and Shani Stajnrod discovered that a flaw in the resolver code can cause named to spend excessive amounts of time on processing large delegations, significantly degrade resolver performance and result in denial of service.

CVE-2022-38177

It was discovered that the DNSSEC verification code for the ECDSA algorithm is susceptible to a memory leak flaw. A remote attacker can take advantage of this flaw to cause BIND to consume resources, resulting in a denial of service.

CVE-2022-38178

It was discovered that the DNSSEC verification code for the EdDSA algorithm is susceptible to a memory leak flaw. A remote attacker can take advantage of this flaw to cause BIND to consume resources, resulting in a denial of service.

For Debian 10 buster, these problems have been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u8.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/bind9

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/bind9
https://security-tracker.debian.org/tracker/CVE-2022-2795
https://security-tracker.debian.org/tracker/CVE-2022-38177
https://security-tracker.debian.org/tracker/CVE-2022-38178
https://packages.debian.org/source/buster/bind9

Solution

Upgrade the bind9 packages.

Risk Factor

High

CVSS v4.0 Base Score

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

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-2795
CVE	CVE-2022-38177
CVE	CVE-2022-38178
XREF	IAVA:2022-A-0387-S

Plugin Information

Published: 2022/10/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u8
```

166426 - Debian dla-3152 : glibc-doc - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3152 advisory.

---------- Debian LTS Advisory DLA-3152-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Helmut Grohne October 17, 2022 https://wiki.debian.org/LTS

Package : glibc Version : 2.28-10+deb10u2 CVE ID : CVE-2016-10228 CVE-2019-19126 CVE-2019-25013 CVE-2020-1752 CVE-2020-6096 CVE-2020-10029 CVE-2020-27618 CVE-2021-3326 CVE-2021-3999 CVE-2021-27645 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219 Debian Bug : 856503 945250 953108 953788 961452 973914 979273 981198 983479 989147 990542

This update fixes a wide range of vulnerabilities. A significant portion affects character set conversion.

CVE-2016-10228

The iconv program in the GNU C Library when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.

CVE-2019-19126

On the x86-64 architecture, the GNU C Library fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.

CVE-2019-25013

The iconv feature in the GNU C Library, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.

CVE-2020-10029

The GNU C Library could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.

CVE-2020-1752

A use-after-free vulnerability introduced in glibc was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution.

CVE-2020-27618

The iconv function in the GNU C Library, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.

CVE-2020-6096

An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.

CVE-2021-27645

The nameserver caching daemon (nscd) in the GNU C Library, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.

CVE-2021-3326

The iconv function in the GNU C Library, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

CVE-2021-33574

The mq_notify function in the GNU C Library has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.

CVE-2021-35942

The wordexp function in the GNU C Library may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.

CVE-2021-3999

An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and escalate their privileges on the system.

CVE-2022-23218

The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

CVE-2022-23219

The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

For Debian 10 buster, these problems have been fixed in version 2.28-10+deb10u2.

We recommend that you upgrade your glibc packages.

For the detailed security status of glibc please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glibc

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/glibc
https://security-tracker.debian.org/tracker/CVE-2016-10228
https://security-tracker.debian.org/tracker/CVE-2019-19126
https://security-tracker.debian.org/tracker/CVE-2019-25013
https://security-tracker.debian.org/tracker/CVE-2020-10029

https://security-tracker.debian.org/tracker/CVE-2020-1752
https://security-tracker.debian.org/tracker/CVE-2020-27618
https://security-tracker.debian.org/tracker/CVE-2020-6096
https://security-tracker.debian.org/tracker/CVE-2021-27645
https://security-tracker.debian.org/tracker/CVE-2021-3326
https://security-tracker.debian.org/tracker/CVE-2021-33574
https://security-tracker.debian.org/tracker/CVE-2021-35942
https://security-tracker.debian.org/tracker/CVE-2021-3999
https://security-tracker.debian.org/tracker/CVE-2022-23218
https://security-tracker.debian.org/tracker/CVE-2022-23219
https://packages.debian.org/source/buster/glibc

Solution

Upgrade the glibc-doc packages.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-10228
CVE	CVE-2019-19126
CVE	CVE-2019-25013
CVE	CVE-2020-1752
CVE	CVE-2020-6096
CVE	CVE-2020-10029
CVE	CVE-2020-27618
CVE	CVE-2021-3326
CVE	CVE-2021-3999
CVE	CVE-2021-27645
CVE	CVE-2021-33574
CVE	CVE-2021-35942
CVE	CVE-2022-23218
CVE	CVE-2022-23219

Plugin Information

Published: 2022/10/23, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libc-bin_2.28-10
Should be : libc-bin_2.28-10+deb10u2
Remote package installed : libc-l10n_2.28-10
Should be : libc-l10n_2.28-10+deb10u2
Remote package installed : libc6_2.28-10
Should be : libc6_2.28-10+deb10u2
Remote package installed : locales_2.28-10
Should be : locales_2.28-10+deb10u2
```

166562 - Debian dla-3161 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3161 advisory.

- ---------- Debian LTS Advisory DLA-3161-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 26, 2022 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2021a-0+deb10u8

This update includes the changes in tzdata 2022e. Notable changes are:

- - Syria and Jordan are abandoning the DST regime and are changing to permanent +03, so they will not fall back from +03 to +02 on 2022-10-28.

For Debian 10 buster, this problem has been fixed in version 2021a-0+deb10u8.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2022/10/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
Should be : tzdata_2021a-0+deb10u8
```

166671 - Debian dla-3165 : expat - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3165 advisory.

- ---------- Debian LTS Advisory DLA-3165-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Utkarsh Gupta October 28, 2022 https://wiki.debian.org/LTS
- ----------

Package : expat Version : 2.2.6-2+deb10u6 CVE ID : CVE-2022-43680 Debian Bug : 1022743

In src:expat, an XML parsing C library, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.

For Debian 10 buster, this problem has been fixed in version 2.2.6-2+deb10u6.

We recommend that you upgrade your expat packages.

For the detailed security status of expat please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/expat

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/expat
https://security-tracker.debian.org/tracker/CVE-2022-43680
https://packages.debian.org/source/buster/expat

Solution

Upgrade the expat packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-43680

Plugin Information

Published: 2022/10/28, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.6-2+deb10u1
Should be : libexpat1_2.2.6-2+deb10u6
```

166734 - Debian dla-3172 : libxml2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3172 advisory.

---------- Debian LTS Advisory DLA-3172-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany October 30, 2022 https://wiki.debian.org/LTS

Package : libxml2 Version : 2.9.4+dfsg1-7+deb10u5 CVE ID : CVE-2022-40303 CVE-2022-40304 Debian Bug : 1022224 1022225

It was discovered that libxml2, the GNOME XML library, was vulnerable to integer overflows and memory corruption.

CVE-2022-40303

Parsing a XML document with the XML_PARSE_HUGE option enabled can result in an integer overflow because safety checks were missing in some functions. Also, the xmlParseEntityValue function did not have any length limitation.

CVE-2022-40304

When a reference cycle is detected in the XML entity cleanup function the XML entity data can be stored in a dictionary. In this case, the dictionary becomes corrupted resulting in logic errors, including memory errors like double free.

For Debian 10 buster, these problems have been fixed in version 2.9.4+dfsg1-7+deb10u5.

We recommend that you upgrade your libxml2 packages.

For the detailed security status of libxml2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libxml2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libxml2
https://security-tracker.debian.org/tracker/CVE-2022-40303
https://security-tracker.debian.org/tracker/CVE-2022-40304
https://packages.debian.org/source/buster/libxml2

Solution

Upgrade the libxml2 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-40303
CVE	CVE-2022-40304

Plugin Information

Published: 2022/10/31, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-7+deb10u1
Should be : libxml2_2.9.4+dfsg1-7+deb10u5
```

167748 - Debian dla-3190 : grub-common - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3190 advisory.

- ---------- Debian LTS Advisory DLA-3190-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Steve

McIntyre November 16, 2022 https://wiki.debian.org/LTS
- --

Package : grub2 Version : 2.06-3~deb10u2 CVE ID : CVE-2022-2601 CVE-2022-3775

Several issues were found in GRUB2's font handling code, which could result in crashes and potentially execution of arbitrary code. These could lead to by-pass of UEFI Secure Boot on affected systems.

Further, issues were found in image loading that could potentially lead to memory overflows.

For Debian 10 buster, these problems have been fixed in version 2.06-3~deb10u2.

We recommend that you upgrade your grub2 packages.

For the detailed security status of grub2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/grub2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/grub2
https://security-tracker.debian.org/tracker/CVE-2022-2601
https://security-tracker.debian.org/tracker/CVE-2022-3775
https://packages.debian.org/source/buster/grub2

Solution

Upgrade the grub-common packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2601
CVE	CVE-2022-3775

Plugin Information

Published: 2022/11/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : grub-common_2.02+dfsg1-20+deb10u4
Should be : grub-common_2.06-3~deb10u2
Remote package installed : grub-pc_2.02+dfsg1-20+deb10u4
Should be : grub-pc_2.06-3~deb10u2
Remote package installed : grub-pc-bin_2.02+dfsg1-20+deb10u4
Should be : grub-pc-bin_2.06-3~deb10u2
Remote package installed : grub2-common_2.02+dfsg1-20+deb10u4
Should be : grub2-common_2.06-3~deb10u2
```

168183 - Debian dla-3204 : vim - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3204 advisory.

---------- Debian LTS Advisory DLA-3204-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Helmut Grohne November 24, 2022 https://wiki.debian.org/LTS

Package : vim Version : 2:8.1.0875-5+deb10u4 CVE ID : CVE-2022-0318 CVE-2022-0392 CVE-2022-0629 CVE-2022-0696 CVE-2022-1619 CVE-2022-1621 CVE-2022-1785 CVE-2022-1897 CVE-2022-1942 CVE-2022-2000 CVE-2022-2129 CVE-2022-3235 CVE-2022-3256 CVE-2022-3352

This update fixes multiple memory access violations in vim.

CVE-2022-0318

Heap-based Buffer Overflow

CVE-2022-0392

Heap-based Buffer Overflow

CVE-2022-0629

Stack-based Buffer Overflow

CVE-2022-0696

NULL Pointer Dereference

CVE-2022-1619

Heap-based Buffer Overflow in function cmdline_erase_chars. This vulnerabilities are capable of crashing software, modify memory, and possible remote execution

CVE-2022-1621

Heap buffer overflow in vim_strncpy find_word. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution

CVE-2022-1785

Out-of-bounds Write

CVE-2022-1897

Out-of-bounds Write

CVE-2022-1942

Heap-based Buffer Overflow

CVE-2022-2000

Out-of-bounds Write

CVE-2022-2129

Out-of-bounds Write

CVE-2022-3235

Use After Free

CVE-2022-3256

Use After Free

CVE-2022-3352

Use After Free

For Debian 10 buster, these problems have been fixed in version 2:8.1.0875-5+deb10u4.

We recommend that you upgrade your vim packages.

For the detailed security status of vim please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/vim

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/vim
https://security-tracker.debian.org/tracker/CVE-2022-0318
https://security-tracker.debian.org/tracker/CVE-2022-0392
https://security-tracker.debian.org/tracker/CVE-2022-0629
https://security-tracker.debian.org/tracker/CVE-2022-0696
https://security-tracker.debian.org/tracker/CVE-2022-1619
https://security-tracker.debian.org/tracker/CVE-2022-1621
https://security-tracker.debian.org/tracker/CVE-2022-1785
https://security-tracker.debian.org/tracker/CVE-2022-1897
https://security-tracker.debian.org/tracker/CVE-2022-1942
https://security-tracker.debian.org/tracker/CVE-2022-2000
https://security-tracker.debian.org/tracker/CVE-2022-2129
https://security-tracker.debian.org/tracker/CVE-2022-3235
https://security-tracker.debian.org/tracker/CVE-2022-3256
https://security-tracker.debian.org/tracker/CVE-2022-3352
https://packages.debian.org/source/buster/vim

Solution

Upgrade the vim packages.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0318
CVE	CVE-2022-0392
CVE	CVE-2022-0629
CVE	CVE-2022-0696
CVE	CVE-2022-1619
CVE	CVE-2022-1621
CVE	CVE-2022-1785
CVE	CVE-2022-1897
CVE	CVE-2022-1942
CVE	CVE-2022-2000
CVE	CVE-2022-2129
CVE	CVE-2022-3235
CVE	CVE-2022-3256
CVE	CVE-2022-3352

Plugin Information

Published: 2022/11/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
  Remote package installed : vim-common_2:8.1.0875-5
  Should be : vim-common_2:8.1.0875-5+deb10u4
  Remote package installed : vim-tiny_2:8.1.0875-5
  Should be : vim-tiny_2:8.1.0875-5+deb10u4
  Remote package installed : xxd_2:8.1.0875-5
  Should be : xxd_2:8.1.0875-5+deb10u4
```

168264 - Debian dla-3213 : krb5-admin-server - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3213 advisory.

- ---------- Debian LTS Advisory DLA-3213-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb November 29, 2022 https://wiki.debian.org/LTS
- ----------

Package : krb5 Version : 1.17-3+deb10u5 CVE ID : CVE-2022-42898 Debian Bug : 1024267

It was discovered that there was a potential Denial of Service (DoS) attack against krb5, a suite of tools implementing the Kerberos authentication system. An integer overflow in PAC parsing could have been exploited if a cross-realm entity acted maliciously.

For Debian 10 buster, this problem has been fixed in version 1.17-3+deb10u5.

We recommend that you upgrade your krb5 packages.

For the detailed security status of krb5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/krb5

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/CVE-2022-42898
https://security-tracker.debian.org/tracker/source-package/krb5
https://packages.debian.org/source/buster/krb5

Solution

Upgrade the krb5-admin-server packages.

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)

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)

References

CVE CVE-2022-42898

Plugin Information

Published: 2022/11/29, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : krb5-locales_1.17-3+deb10u1
Should be : krb5-locales_1.17-3+deb10u5
Remote package installed : libgssapi-krb5-2_1.17-3+deb10u1
Should be : libgssapi-krb5-2_1.17-3+deb10u5
Remote package installed : libk5crypto3_1.17-3+deb10u1
Should be : libk5crypto3_1.17-3+deb10u5
Remote package installed : libkrb5-3_1.17-3+deb10u1
Should be : libkrb5-3_1.17-3+deb10u5
Remote package installed : libkrb5support0_1.17-3+deb10u1
Should be : libkrb5support0_1.17-3+deb10u5
```

169736 - Debian dla-3263 : libtasn1-6 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3263 advisory.

- ---------- Debian LTS Advisory DLA-3263-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb January 09, 2023 https://wiki.debian.org/LTS
- ----------

Package : libtasn1-6 Version : 4.13-3+deb10u1 CVE ID : CVE-2021-46848

It was discovered that there was an off-by-one array size issue in libtasn1-6, a library to manage the generic ASN.1 data structure.

For Debian 10 buster, this problem has been fixed in version 4.13-3+deb10u1.

We recommend that you upgrade your libtasn1-6 packages.

For the detailed security status of libtasn1-6 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libtasn1-6

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/CVE-2021-46848
https://security-tracker.debian.org/tracker/source-package/libtasn1-6
https://packages.debian.org/source/buster/libtasn1-6

Solution

Upgrade the libtasn1-6 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-46848

Plugin Information

Published: 2023/01/10, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libtasn1-6_4.13-3
Should be : libtasn1-6_4.13-3+deb10u1
```

171626 - Debian dla-3321 : gnutls-bin - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3321 advisory.

---------- Debian LTS Advisory DLA-3321-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany February 18, 2023 https://wiki.debian.org/LTS

Package : gnutls28 Version : 3.6.7-4+deb10u10 CVE ID : CVE-2023-0361

Hubert Kario discovered a timing side channel in the RSA decryption implementation of the GNU TLS library.

For Debian 10 buster, this problem has been fixed in version 3.6.7-4+deb10u10.

We recommend that you upgrade your gnutls28 packages.

For the detailed security status of gnutls28 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/gnutls28

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/gnutls28
https://security-tracker.debian.org/tracker/CVE-2023-0361
https://packages.debian.org/source/buster/gnutls28

Solution

Upgrade the gnutls-bin packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-0361

Plugin Information

Published: 2023/02/18, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libgnutls30_3.6.7-4+deb10u6
Should be : libgnutls30_3.6.7-4+deb10u10
```

214477 - Debian dla-3326 : isc-dhcp-client - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3326 advisory.

---------- Debian LTS Advisory DLA-3326-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastian Blank February 20, 2023 https://wiki.debian.org/LTS

Package : isc-dhcp Version : 4.4.1-2+deb10u3 Debian Bug : 1022969

Under not completely understood conditions, dhclient completely removes IPv6 addresses from use and is unable to restore them.

For Debian 10 buster, this problem has been fixed in version 4.4.1-2+deb10u3.

We recommend that you upgrade your isc-dhcp packages.

For the detailed security status of isc-dhcp please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/isc-dhcp

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/isc-dhcp
https://packages.debian.org/source/buster/isc-dhcp

Solution

Upgrade the isc-dhcp-client packages.

Risk Factor

High

Plugin Information

Published: 2025/01/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : isc-dhcp-client_4.4.1-2
Should be : isc-dhcp-client_4.4.1-2+deb10u3
Remote package installed : isc-dhcp-common_4.4.1-2
Should be : isc-dhcp-common_4.4.1-2+deb10u3
```

171870 - Debian dla-3338 : git - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3338 advisory.

- ---------- Debian LTS Advisory DLA-3338-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort February 23, 2023 https://wiki.debian.org/LTS
- ----------

Package : git Version : 1:2.20.1-2+deb10u8 CVE ID : CVE-2023-22490 CVE-2023-23946

Several vulnerabilities have been discovered in git, a fast, scalable and distributed revision control system.

CVE-2023-22490

yvvdwf found a data exfiltration vulnerability while performing a local clone from a malicious repository even using a non-local transport.

CVE-2023-23946

Joern Schneeweisz found a path traversal vulnerbility in git-apply that a path outside the working tree can be overwritten as the acting user.

For Debian 10 buster, these problems have been fixed in version 1:2.20.1-2+deb10u8.

We recommend that you upgrade your git packages.

For the detailed security status of git please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/git

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/git
https://security-tracker.debian.org/tracker/CVE-2023-22490
https://security-tracker.debian.org/tracker/CVE-2023-23946
https://packages.debian.org/source/buster/git

Solution

Upgrade the git packages.

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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22490
CVE	CVE-2023-23946

Plugin Information

Published: 2023/02/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : git_1:2.20.1-2+deb10u3
Should be : git_1:2.20.1-2+deb10u8
Remote package installed : git-man_1:2.20.1-2+deb10u3
Should be : git-man_1:2.20.1-2+deb10u8
```

171901 - Debian dla-3341 : curl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3341 advisory.

- ---------- Debian LTS Advisory DLA-3341-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk February 24, 2023 https://wiki.debian.org/LTS
- ----------

Package : curl Version : 7.64.0-4+deb10u5 CVE ID : CVE-2023-23916 Debian Bug : 1031371

HTTP multi-header compression denial of service has been fixed in curl, a command line tool and library for transferring data with URLs.

For Debian 10 buster, this problem has been fixed in version 7.64.0-4+deb10u5.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2023-23916
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-23916
XREF	IAVA:2023-A-0008-S

Plugin Information

Published: 2023/02/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u5
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u5
```

173399 - Debian dla-3366 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3366 advisory.

- ---------- Debian LTS Advisory DLA-3366-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort March 24, 2023 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2021a-0+deb10u10

This update includes the changes in tzdata 2023b. Notable changes are:

- - Egypt uses DST again, starting on April.
- - Palestine and Lebanon delay the start of DST this year.
- - Morocco DST will happen a week earlier on April 23.
- - Adjustments to Greenland's timezones and DST rules.

For Debian 10 buster, this problem has been fixed in version 2021a-0+deb10u10.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2023/03/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
Should be : tzdata_2021a-0+deb10u10
```

174964 - Debian dla-3405 : libxml2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3405 advisory.

- ---------- Debian LTS Advisory DLA-3405-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz April 30, 2023 https://wiki.debian.org/LTS
- ----------

Package : libxml2 Version : 2.9.4+dfsg1-7+deb10u6 CVE ID : CVE-2023-28484 CVE-2023-29469

Several vulnerabilities were discovered in libxml2, a library providing support to read, modify and write XML and HTML files.

CVE-2023-28484

A NULL pointer dereference flaw when parsing invalid XML schemas may result in denial of service.

CVE-2023-29469

It was reported that when hashing empty strings which aren't null-terminated, xmlDictComputeFastKey could produce inconsistent results, which may lead to various logic or memory errors.

For Debian 10 buster, these problems have been fixed in version 2.9.4+dfsg1-7+deb10u6.

We recommend that you upgrade your libxml2 packages.

For the detailed security status of libxml2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libxml2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libxml2
https://security-tracker.debian.org/tracker/CVE-2023-28484
https://security-tracker.debian.org/tracker/CVE-2023-29469
https://packages.debian.org/source/buster/libxml2

Solution

Upgrade the libxml2 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-28484
CVE	CVE-2023-29469

Plugin Information

Published: 2023/05/01, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-7+deb10u1
Should be : libxml2_2.9.4+dfsg1-7+deb10u6
```

175048 - Debian dla-3412 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3412 advisory.

- ---------- Debian LTS Advisory DLA-3412-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort May 02, 2023 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2021a-0+deb10u11

This update includes the changes in tzdata 2023c. Notable changes are:

- - Revert Lebanon DST changes.
- - Updated leap second list.

For Debian 10 buster, this problem has been fixed in version 2021a-0+deb10u11.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2023/05/03, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
Should be : tzdata_2021a-0+deb10u11
```

176347 - Debian dla-3432 : idle-python2.7 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3432 advisory.

- ---------- Debian LTS Advisory DLA-3432-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler May 24, 2023 https://wiki.debian.org/LTS
- ----------

Package : python2.7 Version : 2.7.16-2+deb10u2 CVE ID : CVE-2015-20107 CVE-2019-20907 CVE-2020-8492 CVE-2020-26116 CVE-2021-3177 CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2022-45061 Debian Bug : 970099

Multiple security issues were discovered in Python, an interactive high-level object-oriented language. An attacker may cause command injection, denial of service (DoS), request smuggling and port scanning.

CVE-2015-20107

The mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments).

CVE-2019-20907

In Lib/tarfile.py, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.

CVE-2020-8492

Python allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.

CVE-2020-26116

http.client allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.

CVE-2021-3177

Python has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

CVE-2021-3733

There's a flaw in urllib's AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client.

CVE-2021-3737

An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time.

CVE-2021-4189

The FTP (File Transfer Protocol) client library in PASV (passive) mode trusts the host from the PASV response by default. This flaw allows an attacker to set up a malicious FTP server that can trick FTP clients into connecting back to a given IP address and port. This vulnerability could lead to FTP client scanning ports. For the rare user who wants the previous behavior, set a `trust_server_pasv_ipv4_address` attribute on your `ftplib.FTP` instance to True.

CVE-2022-45061

An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service.

For Debian 10 buster, these problems have been fixed in version 2.7.16-2+deb10u2.

We recommend that you upgrade your python2.7 packages.

For the detailed security status of python2.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python2.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python2.7
https://security-tracker.debian.org/tracker/CVE-2015-20107
https://security-tracker.debian.org/tracker/CVE-2019-20907
https://security-tracker.debian.org/tracker/CVE-2020-26116
https://security-tracker.debian.org/tracker/CVE-2020-8492
https://security-tracker.debian.org/tracker/CVE-2021-3177
https://security-tracker.debian.org/tracker/CVE-2021-3733
https://security-tracker.debian.org/tracker/CVE-2021-3737
https://security-tracker.debian.org/tracker/CVE-2021-4189
https://security-tracker.debian.org/tracker/CVE-2022-45061
https://packages.debian.org/source/buster/python2.7

Solution

Upgrade the idle-python2.7 packages.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-20107
CVE	CVE-2019-20907
CVE	CVE-2020-8492
CVE	CVE-2020-26116
CVE	CVE-2021-3177
CVE	CVE-2021-3733
CVE	CVE-2021-3737
CVE	CVE-2021-4189
CVE	CVE-2022-45061

Plugin Information

Published: 2023/05/25, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.16-2+deb10u1
Should be : libpython2.7-minimal_2.7.16-2+deb10u2
Remote package installed : libpython2.7-stdlib_2.7.16-2+deb10u1
Should be : libpython2.7-stdlib_2.7.16-2+deb10u2
Remote package installed : python2.7_2.7.16-2+deb10u1
```

```
Should be : python2.7_2.7.16-2+deb10u2
Remote package installed : python2.7-minimal_2.7.16-2+deb10u1
Should be : python2.7-minimal_2.7.16-2+deb10u2
```

177218 - Debian dla-3453 : vim - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3453 advisory.

---------- Debian LTS Advisory DLA-3453-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany June 12, 2023 https://wiki.debian.org/LTS

Package : vim Version : 2:8.1.0875-5+deb10u5 CVE ID : CVE-2022-4141 CVE-2023-0054 CVE-2023-1175 CVE-2023-2610 Debian Bug : 1027146 1031875 1035955

Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows and out-of-bounds reads may lead to a denial-of-service (application crash) or other unspecified impact.

For Debian 10 buster, these problems have been fixed in version 2:8.1.0875-5+deb10u5.

We recommend that you upgrade your vim packages.

For the detailed security status of vim please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/vim

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/vim
https://security-tracker.debian.org/tracker/CVE-2022-4141
https://security-tracker.debian.org/tracker/CVE-2023-0054
https://security-tracker.debian.org/tracker/CVE-2023-1175
https://security-tracker.debian.org/tracker/CVE-2023-2610
https://packages.debian.org/source/buster/vim

Solution

Upgrade the vim packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-4141
CVE	CVE-2023-0054
CVE	CVE-2023-1175
CVE	CVE-2023-2610
XREF	IAVB:2022-B-0058-S
XREF	IAVB:2023-B-0016-S
XREF	IAVB:2023-B-0018-S
XREF	IAVB:2023-B-0033-S

Plugin Information

Published: 2023/06/13, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.1.0875-5
Should be : vim-common_2:8.1.0875-5+deb10u5
Remote package installed : vim-tiny_2:8.1.0875-5
Should be : vim-tiny_2:8.1.0875-5+deb10u5
Remote package installed : xxd_2:8.1.0875-5
Should be : xxd_2:8.1.0875-5+deb10u5
```

177636 - Debian dla-3472 : libx11-6 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3472 advisory.

- ---------- Debian LTS Advisory DLA-3472-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 26, 2023 https://wiki.debian.org/LTS
- ----------

Package : libx11 Version : 2:1.6.7-1+deb10u3 CVE ID : CVE-2023-3138 Debian Bug : 1038133

Missing input validation in various functions may have resulted in denial of service in various functions provided by libx11, the X11 client-side library.

For Debian 10 buster, this problem has been fixed in version 2:1.6.7-1+deb10u3.

We recommend that you upgrade your libx11 packages.

For the detailed security status of libx11 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libx11

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libx11
https://security-tracker.debian.org/tracker/CVE-2023-3138
https://packages.debian.org/source/buster/libx11

Solution

Upgrade the libx11-6 packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-3138

Plugin Information

Published: 2023/06/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.7-1+deb10u1
Should be : libx11-6_2:1.6.7-1+deb10u3
Remote package installed : libx11-data_2:1.6.7-1+deb10u1
Should be : libx11-data_2:1.6.7-1+deb10u3
```

177875 - Debian dla-3477 : idle-python3.7 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3477 advisory.

- ---------- Debian LTS Advisory DLA-3477-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 30, 2023 https://wiki.debian.org/LTS
- ----------

Package : python3.7 Version : 3.7.3-2+deb10u5 CVE ID : CVE-2015-20107 CVE-2020-10735 CVE-2021-3426 CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2022-45061

Several vulnerabilities were fixed in the Python3 interpreter.

CVE-2015-20107

The mailcap module did not add escape characters into commands discovered in the system mailcap file.

CVE-2020-10735

Prevent DoS with very large int.

CVE-2021-3426

Remove the pydoc getfile feature which could be abused to read arbitrary files on the disk.

CVE-2021-3733

Regular Expression Denial of Service in urllib's AbstractBasicAuthHandler class.

CVE-2021-3737

Infinite loop in the HTTP client code.

CVE-2021-4189

Make ftplib not trust the PASV response.

CVE-2022-45061

Quadratic time in the IDNA decoder.

For Debian 10 buster, these problems have been fixed in version 3.7.3-2+deb10u5.

We recommend that you upgrade your python3.7 packages.

For the detailed security status of python3.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python3.7
https://security-tracker.debian.org/tracker/CVE-2015-20107
https://security-tracker.debian.org/tracker/CVE-2020-10735
https://security-tracker.debian.org/tracker/CVE-2021-3426
https://security-tracker.debian.org/tracker/CVE-2021-3733
https://security-tracker.debian.org/tracker/CVE-2021-3737
https://security-tracker.debian.org/tracker/CVE-2021-4189
https://security-tracker.debian.org/tracker/CVE-2022-45061
https://packages.debian.org/source/buster/python3.7

Solution

Upgrade the idle-python3.7 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-20107
CVE	CVE-2020-10735
CVE	CVE-2021-3426
CVE	CVE-2021-3733
CVE	CVE-2021-3737
CVE	CVE-2021-4189
CVE	CVE-2022-45061

Plugin Information

Published: 2023/07/01, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython3.7-minimal_3.7.3-2+deb10u2
Should be : libpython3.7-minimal_3.7.3-2+deb10u5
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u2
Should be : libpython3.7-stdlib_3.7.3-2+deb10u5
Remote package installed : python3.7_3.7.3-2+deb10u2
Should be : python3.7_3.7.3-2+deb10u5
Remote package installed : python3.7-minimal_3.7.3-2+deb10u2
Should be : python3.7-minimal_3.7.3-2+deb10u5
```

178638 - Debian dla-3482 : debian-archive-keyring - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3482 advisory.

---------- Debian LTS Advisory DLA-3482-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Jochen Sprickerhof July 07, 2023 https://wiki.debian.org/LTS

Package : debian-archive-keyring Version : 2019.1+deb10u2 CVE ID :
Debian Bug :

debian-archive-keyring is a package containing GnuPG archive keys of the Debian archive. New GPG-keys are being constantly added with every new Debian release.

For Debian 10 buster, GPG-keys for 12/bullseye Debian release are added in the version 2019.1+deb10u2.

We recommend that you upgrade your debian-archive-keyring packages only if you need to work with packages from 12/bullseye release.

For the detailed security status of debian-archive-keyring please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/debian-archive-keyring

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

http://www.nessus.org/u?fdde0805
https://packages.debian.org/source/buster/debian-archive-keyring

Solution

Upgrade the debian-archive-keyring packages.

Risk Factor

High

Plugin Information

Published: 2023/07/20, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : debian-archive-keyring_2019.1
Should be : debian-archive-keyring_2019.1+deb10u2
```

178479 - Debian dla-3498 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3498 advisory.

- ---------- Debian LTS Advisory DLA-3498-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb July 18, 2023 https://wiki.debian.org/LTS
- ----------

Package : bind9 Version : 1:9.11.5.P4+dfsg-5.1+deb10u9 CVE ID : CVE-2023-2828

It was discovered that there was a potential denial of service (DoS) in bind9, the popular Domain Name Server (DNS) server.

Shoham Danino, Anat Bremler-Barr, Yehuda Afek and Yuval Shavitt discovered that a flaw in the cache-cleaning algorithm used in named can cause that named's configured cache size limit can be significantly exceeded, potentially resulting in a denial of service attack.

For Debian 10 buster, this problem has been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u9.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/bind9

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/CVE-2023-2828
https://security-tracker.debian.org/tracker/source-package/bind9
https://packages.debian.org/source/buster/bind9

Solution

Upgrade the bind9 packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2828
XREF	IAVA:2023-A-0320-S

Plugin Information

Published: 2023/07/19, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u9
```

182157 - Debian dla-3586 : lib32ncurses-dev - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3586 advisory.

---------- Debian LTS Advisory DLA-3586-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton September 28, 2023 https://wiki.debian.org/LTS

Package : ncurses Version : 6.1+20181013-2+deb10u4 CVE ID : CVE-2020-19189

An out-of-bounds read problem was found in the postprocess_terminfo function of ncurses, a text-based user interface toolkit, which could potentially lead to an exposure of sensitive information or denial of service.

For Debian 10 buster, these problems have been fixed in version 6.1+20181013-2+deb10u4.

We recommend that you upgrade your ncurses packages.

For the detailed security status of ncurses please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/ncurses

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/ncurses
https://security-tracker.debian.org/tracker/CVE-2020-19189
https://packages.debian.org/source/buster/ncurses

Solution

Upgrade the lib32ncurses-dev packages.

Risk Factor

High

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-19189

Plugin Information

Published: 2023/09/28, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libncurses6_6.1+20181013-2+deb10u2
Should be : libncurses6_6.1+20181013-2+deb10u4
Remote package installed : libncursesw6_6.1+20181013-2+deb10u2
Should be : libncursesw6_6.1+20181013-2+deb10u4
Remote package installed : libtinfo6_6.1+20181013-2+deb10u2
Should be : libtinfo6_6.1+20181013-2+deb10u4
Remote package installed : ncurses-base_6.1+20181013-2+deb10u2
Should be : ncurses-base_6.1+20181013-2+deb10u4
Remote package installed : ncurses-bin_6.1+20181013-2+deb10u2
Should be : ncurses-bin_6.1+20181013-2+deb10u4
```

```
Remote package installed : ncurses-term_6.1+20181013-2+deb10u2
Should be : ncurses-term_6.1+20181013-2+deb10u4
```

182369 - Debian dla-3588 : vim - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3588 advisory.

- ---------- Debian LTS Advisory DLA-3588-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris September 29, 2023 https://wiki.debian.org/LTS
- ----------

Package : vim Version : 2:8.1.0875-5+deb10u6 CVE ID : CVE-2023-4752 CVE-2023-4781

Multiple vulnerabilities were found in vim a text editor.

CVE-2023-4752

A heap use after free was found in ins_compl_get_exp()

CVE-2023-4781

A heap-buffer-overflow was found in vim_regsub_both()

For Debian 10 buster, these problems have been fixed in version 2:8.1.0875-5+deb10u6.

We recommend that you upgrade your vim packages.

For the detailed security status of vim please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/vim

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/vim
https://security-tracker.debian.org/tracker/CVE-2023-4752
https://security-tracker.debian.org/tracker/CVE-2023-4781
https://packages.debian.org/source/buster/vim

Solution

Upgrade the vim packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-4752
CVE	CVE-2023-4781
XREF	IAVB:2023-B-0066-S

Plugin Information

Published: 2023/09/29, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.1.0875-5
Should be : vim-common_2:8.1.0875-5+deb10u6
Remote package installed : vim-tiny_2:8.1.0875-5
Should be : vim-tiny_2:8.1.0875-5+deb10u6
Remote package installed : xxd_2:8.1.0875-5
Should be : xxd_2:8.1.0875-5+deb10u6
```

186663 - Debian dla-3684 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3684 advisory.

- ---------- Debian LTS Advisory DLA-3684-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort December 07, 2023 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2021a-0+deb10u12 Debian Bug : 1036104 1057185 1057186

This update includes the latest changes to the leap second list, including an update to its expiry date, which was set for the end of December.

For Debian 10 buster, this problem has been fixed in version 2021a-0+deb10u12.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2023/12/07, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
```

```
Should be : tzdata_2021a-0+deb10u12
```

189836 - Debian dla-3726 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3726 advisory.

- ---------- Debian LTS Advisory DLA-3726-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz January 30, 2024 https://wiki.debian.org/LTS
- ----------

Package : bind9 Version : 1:9.11.5.P4+dfsg-5.1+deb10u10 CVE ID : CVE-2023-3341

An issue has been discovered in BIND, a DNS server implementation.

A stack exhaustion flaw was discovered in the control channel code which may result in denial of service (named daemon crash).

For Debian 10 buster, this problem has been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u10.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/bind9

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/bind9
https://security-tracker.debian.org/tracker/CVE-2023-3341
https://packages.debian.org/source/buster/bind9

Solution

Upgrade the bind9 packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3341
XREF	IAVA:2023-A-0500-S

Plugin Information

Published: 2024/01/31, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u10
```

189972 - Debian dla-3732 : sudo - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3732 advisory.

- ---------- Debian LTS Advisory DLA-3732-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris February 03, 2024 https://wiki.debian.org/LTS
- ----------

Package : sudo Version : 1.8.27-1+deb10u6 CVE ID : CVE-2023-7090 CVE-2023-28486 CVE-2023-28487

Sudo, a program designed to allow a sysadmin to give limited root privileges to users and log root activity, was vulnerable.

CVE-2023-7090

A flaw was found in sudo in the handling of ipa_hostname, where ipa_hostname from /etc/sssd/sssd.conf was not propagated in sudo.
Therefore, it leads to privilege mismanagement vulnerability in applications, where client hosts retain privileges even after retracting them.

CVE-2023-28486

Sudo did not escape control characters in log messages.

CVE-2023-28487

Sudo did not escape control characters in sudoreplay output.

For Debian 10 buster, these problems have been fixed in version 1.8.27-1+deb10u6.

We recommend that you upgrade your sudo packages.

For the detailed security status of sudo please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/sudo

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/sudo
https://security-tracker.debian.org/tracker/CVE-2023-28486
https://security-tracker.debian.org/tracker/CVE-2023-28487
https://security-tracker.debian.org/tracker/CVE-2023-7090
https://packages.debian.org/source/buster/sudo

Solution

Upgrade the sudo packages.

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)

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

II

References

CVE	CVE-2023-7090
CVE	CVE-2023-28486
CVE	CVE-2023-28487
XREF	IAVA:2023-A-0121-S

Plugin Information

Published: 2024/02/03, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.27-1+deb10u3
Should be : sudo_1.8.27-1+deb10u6
```

190998 - Debian dla-3740 : gnutls-bin - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3740 advisory.

---------- Debian LTS Advisory DLA-3740-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin February 26, 2024 https://wiki.debian.org/LTS

Package : gnutls28 Version : 3.6.7-4+deb10u12 CVE ID : CVE-2024-0553 Debian Bug : 1061046

Hubert Kario discovered that GnuTLS, a portable library which implements the Transport Layer Security and Datagram Transport Layer Security protocols, was vulnerable to timing side-channel attack in the RSA-PSK key exchange, which could lead to leakage of sensitive data. The issue stems from an incomplete resolution for CVE-2023-5981.

This vulnerability is also known as GNUTLS-SA-2024-01-14.

For Debian 10 buster, this problem has been fixed in version 3.6.7-4+deb10u12.

We recommend that you upgrade your gnutls28 packages.

For the detailed security status of gnutls28 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/gnutls28

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/gnutls28
https://security-tracker.debian.org/tracker/CVE-2023-5981
https://security-tracker.debian.org/tracker/CVE-2024-0553
https://packages.debian.org/source/buster/gnutls28

Solution

Upgrade the gnutls-bin packages.

Risk Factor

High

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5981
CVE	CVE-2024-0553

Plugin Information

Published: 2024/02/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libgnutls30_3.6.7-4+deb10u6
Should be : libgnutls30_3.6.7-4+deb10u12
```

191787 - Debian dla-3757 : libnss3 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3757 advisory.

---------- Debian LTS Advisory DLA-3757-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Tobias Frost March 10, 2024 https://wiki.debian.org/LTS

Package : nss Version : 2:3.42.1-1+deb10u8 CVE ID : CVE-2023-5388 CVE-2024-0743 Debian Bug : 1056284

Multiple vulnerabilities were found in nss, a set of libraries designed to support cross-platform development of security-enabled client and server applications.

CVE-2023-5388

Timing attack against RSA decryption in TLS. This vulnerablity has been named The Marvin Attack.

CVE-2024-0743

An unchecked return value in TLS handshake code could have caused a potentially exploitable crash.

For Debian 10 buster, these problems have been fixed in version 2:3.42.1-1+deb10u8.

We recommend that you upgrade your nss packages.

For the detailed security status of nss please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nss

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nss
https://security-tracker.debian.org/tracker/CVE-2023-5388
https://security-tracker.debian.org/tracker/CVE-2024-0743
https://packages.debian.org/source/buster/nss

Solution

Upgrade the libnss3 packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5388
CVE	CVE-2024-0743

Plugin Information

Published: 2024/03/11, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libnss3_2:3.42.1-1+deb10u3
Should be : libnss3_2:3.42.1-1+deb10u8
```

192185 - Debian dla-3763 : curl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3763 advisory.

- ---------- Debian LTS Advisory DLA-3763-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris March 17, 2024 https://wiki.debian.org/LTS
- ----------

Package : curl Version : 7.64.0-4+deb10u9 CVE ID : CVE-2023-27534

curl was affected by a path traversal vulnerability.

SFTP implementation causes the tilde (~) character to be wrongly replaced when used as a prefix in the first path element, in addition to its intended use as the first element to indicate a path relative to the user's home directory. Attackers can exploit this flaw to bypass filtering or execute arbitrary code by crafting a path like /~2/foo while accessing a server with a specific user.

For Debian 10 buster, this problem has been fixed in version 7.64.0-4+deb10u9.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2023-27534
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

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)

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-2023-27534
XREF	IAVA:2023-A-0153-S
XREF	IAVA:2023-A-0531-S

Plugin Information

Published: 2024/03/17, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u9
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u9
```

192520 - Debian dla-3772 : idle-python3.7 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3772 advisory.

- ---------- Debian LTS Advisory DLA-3772-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk March 24, 2024 https://wiki.debian.org/LTS
- ----------

Package : python3.7 Version : 3.7.3-2+deb10u7 CVE ID : CVE-2023-6597 CVE-2024-0450

Two vulnerabilities have been fixed in the Python 3 interpreter.

CVE-2023-6597

tempfile.TemporaryDirectory failure to remove dir

CVE-2024-0450

quoted-overlap zipbomb DoS

For Debian 10 buster, these problems have been fixed in version 3.7.3-2+deb10u7.

We recommend that you upgrade your python3.7 packages.

For the detailed security status of python3.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python3.7
https://security-tracker.debian.org/tracker/CVE-2023-6597
https://security-tracker.debian.org/tracker/CVE-2024-0450
https://packages.debian.org/source/buster/python3.7

Solution

Upgrade the idle-python3.7 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-6597
CVE	CVE-2024-0450

Plugin Information

Published: 2024/03/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython3.7-minimal_3.7.3-2+deb10u2
Should be : libpython3.7-minimal_3.7.3-2+deb10u7
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u2
Should be : libpython3.7-stdlib_3.7.3-2+deb10u7
Remote package installed : python3.7_3.7.3-2+deb10u2
Should be : python3.7_3.7.3-2+deb10u7
Remote package installed : python3.7-minimal_3.7.3-2+deb10u2
Should be : python3.7-minimal_3.7.3-2+deb10u7
```

193076 - Debian dla-3783 : expat - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3783 advisory.

---------- Debian LTS Advisory DLA-3783-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Tobias Frost April 07, 2024 https://wiki.debian.org/LTS

Package : expat Version : 2.2.6-2+deb10u7 CVE ID : CVE-2023-52425 Debian Bug : 1063238

Expat, an XML parsing C library has been found to have an vulnerability that allows an attacker to perform a denial of service (resource consumption, when many full reparsings are required in the case of a large tokens.

When parsing a really big token that requires multiple buffer fills to complete, expat has to re-parse the token from start multiple times, which takes time. These patches introduce a heuristic that, when having failed on the same token multiple times, defers further parsing until there's significantly more data available.

The patch also introduces an optiional API, XML_SetReparseDeferralEnabled(), to disable the new heuristic.

For Debian 10 buster, this problem has been fixed in version 2.2.6-2+deb10u7.

We recommend that you upgrade your expat packages.

For the detailed security status of expat please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/expat

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/expat
https://security-tracker.debian.org/tracker/CVE-2023-52425
https://packages.debian.org/source/buster/expat

Solution

Upgrade the expat packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-52425
XREF	IAVA:2024-A-0134-S

Plugin Information

Published: 2024/04/09, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.6-2+deb10u1
Should be : libexpat1_2.2.6-2+deb10u7
```

193461 - Debian dla-3788 : tzdata - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has a package installed that is affected by a vulnerability as referenced in the dla-3788 advisory.

- ---------- Debian LTS Advisory DLA-3788-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort April 18, 2024 https://wiki.debian.org/LTS
- ----------

Package : tzdata Version : 2024a-0+deb10u1

This update includes the changes in tzdata 2024a. Notable changes are:

- - Kazakhstan unifies on UTC+5 beginning 2024-03-01.
- - Palestine springs forward a week later after Ramadan.

For Debian 10 buster, this problem has been fixed in version 2024a-0+deb10u1.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tzdata
https://packages.debian.org/source/buster/tzdata

Solution

Upgrade the tzdata packages.

Risk Factor

High

Plugin Information

Published: 2024/04/18, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tzdata_2021a-0+deb10u1
Should be : tzdata_2024a-0+deb10u1
```

194852 - Debian dla-3804 : libnghttp2-14 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3804 advisory.

---------- Debian LTS Advisory DLA-3804-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin April 30, 2024 https://wiki.debian.org/LTS

Package : nghttp2 Version : 1.36.0-2+deb10u3 CVE ID : CVE-2024-28182 Debian Bug : 1068415

Bartek Nowotarskis discovered that nghttp2, a set of programs implementing the HTTP/2, keeps reading CONTINUATION frames even after a stream is reset to keep HPACK context in sync. This causes excessive CPU usage to decode HPACK stream, which could lead to Denial of Service.

The issue is mitigated by limiting the number of CONTINUATION frames it can accept after a HEADERS frame. The limit is configurable and defaults to 8.

For Debian 10 buster, this problem has been fixed in version 1.36.0-2+deb10u3.

We recommend that you upgrade your nghttp2 packages.

For the detailed security status of nghttp2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nghttp2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nghttp2
https://security-tracker.debian.org/tracker/CVE-2024-28182
https://packages.debian.org/source/buster/nghttp2

Solution

Upgrade the libnghttp2-14 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28182

Plugin Information

Published: 2024/04/30, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libnghttp2-14_1.36.0-2+deb10u1
Should be : libnghttp2-14_1.36.0-2+deb10u3
```

194968 - Debian dla-3807 : glibc-doc - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3807 advisory.

- ---------- Debian LTS Advisory DLA-3807-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk May 04, 2024 https://wiki.debian.org/LTS
- ----------

Package : glibc Version : 2.28-10+deb10u3 CVE ID : CVE-2024-2961 Debian Bug : 1069191

Out-of-bounds write in the iconv ISO-2022-CN-EXT module has been fixed in the GNU C library.

For Debian 10 buster, this problem has been fixed in version 2.28-10+deb10u3.

We recommend that you upgrade your glibc packages.

For the detailed security status of glibc please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glibc

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/glibc
https://security-tracker.debian.org/tracker/CVE-2024-2961
https://packages.debian.org/source/buster/glibc

Solution

Upgrade the glibc-doc packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2024-2961

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/05/04, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libc-bin_2.28-10
Should be : libc-bin_2.28-10+deb10u3
Remote package installed : libc-l10n_2.28-10
Should be : libc-l10n_2.28-10+deb10u3
Remote package installed : libc6_2.28-10
Should be : libc6_2.28-10+deb10u3
Remote package installed : locales_2.28-10
Should be : locales_2.28-10+deb10u3
```

197488 - Debian dla-3816 : bind9 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3816 advisory.

---------- Debian LTS Advisory DLA-3816-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Santiago Ruano Rincn May 17, 2024 https://wiki.debian.org/LTS

Package : bind9 Version : 1:9.11.5.P4+dfsg-5.1+deb10u11 CVE ID : CVE-2023-50387 CVE-2023-50868 Debian Bug :

Two vulnerabilities were discovered in BIND, a DNS server implementation, which may result in denial of service.

CVE-2023-50387

Certain DNSSEC aspects of the DNS protocol allow remote attackers to cause a denial of service via DNSSEC queries. This is known as the KeyTrap issue.

CVE-2023-50868

The Closest Encloser Proof aspect of the DNS protocol allows remote attackers to cause a denial of service via DNSSEC queries in a random subdomain attack. This is known as the NSEC3 issue.

For Debian 10 buster, these problems have been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u11.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/bind9

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/bind9
https://security-tracker.debian.org/tracker/CVE-2023-50387
https://security-tracker.debian.org/tracker/CVE-2023-50868
https://packages.debian.org/source/buster/bind9

Solution

Upgrade the bind9 packages.

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)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-50387
CVE	CVE-2023-50868
XREF	IAVA:2024-A-0103-S

Plugin Information

Published: 2024/05/17, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u11
```

197941 - Debian dla-3823 : less - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has a package installed that is affected by multiple vulnerabilities as referenced in the dla-3823 advisory.

---------- Debian LTS Advisory DLA-3823-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin May 27, 2024 https://wiki.debian.org/LTS

Package : less Version : 487-0.1+deb10u1 CVE ID : CVE-2022-48624 CVE-2024-32487 Debian Bug : 1064293 1068938

Security vulnerabilities were found in less, a pager program similar to more, which could result in arbitrary command execution when processing files with crafted names.

CVE-2022-48624

It was discovered that LESSCLOSE handling in less did not quote shell metacharacters.

CVE-2024-32487

It was discovered that filenames containing a newline character could result in arbitrary command execution during input preprocessor invocation.

For Debian 10 buster, these problems have been fixed in version 487-0.1+deb10u1.

We recommend that you upgrade your less packages.

For the detailed security status of less please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/less

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:

signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/less
https://security-tracker.debian.org/tracker/CVE-2022-48624
https://security-tracker.debian.org/tracker/CVE-2024-32487
https://packages.debian.org/source/buster/less

Solution

Upgrade the less packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-48624
CVE	CVE-2024-32487

Plugin Information

Published: 2024/05/27, Modified: 2025/03/28

Plugin Output

tcp/0

```
Remote package installed : less_487-0.1+b1
Should be : less_487-0.1+deb10u1
```

201168 - Debian dla-3850 : glibc-doc - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3850 advisory.

- ---------- Debian LTS Advisory DLA-3850-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 30, 2024 https://wiki.debian.org/LTS
- ----------

Package : glibc Version : 2.28-10+deb10u4 CVE ID : CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602

Multiple vulnerabilities have been fixed in the Name Service Cache Daemon that is built by the GNU C library and shipped in the nscd binary package.

CVE-2024-33599

nscd: Stack-based buffer overflow in netgroup cache

CVE-2024-33600

nscd: Null pointer crashes after notfound response

CVE-2024-33601

nscd: Daemon may terminate on memory allocation failure

CVE-2024-33602

nscd: Possible memory corruption

For Debian 10 buster, these problems have been fixed in version 2.28-10+deb10u4.

We recommend that you upgrade your glibc packages.

For the detailed security status of glibc please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glibc

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/glibc
https://security-tracker.debian.org/tracker/CVE-2024-33599
https://security-tracker.debian.org/tracker/CVE-2024-33600
https://security-tracker.debian.org/tracker/CVE-2024-33601
https://security-tracker.debian.org/tracker/CVE-2024-33602
https://packages.debian.org/source/buster/glibc

Solution

Upgrade the glibc-doc packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	IAVA:2025-A-0062

Plugin Information

Published: 2024/06/30, Modified: 2025/03/27

Plugin Output

tcp/0

```
Remote package installed : libc-bin_2.28-10
Should be : libc-bin_2.28-10+deb10u4
```

```
Remote package installed : libc-l10n_2.28-10
Should be : libc-l10n_2.28-10+deb10u4
Remote package installed : libc6_2.28-10
Should be : libc6_2.28-10+deb10u4
Remote package installed : locales_2.28-10
Should be : locales_2.28-10+deb10u4
```

146599 - Debian DSA-4855-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple vulnerabilities have been discovered in OpenSSL, a Secure Sockets Layer toolkit. An overflow bug in the x64_64 Montgomery squaring procedure, an integer overflow in CipherUpdate and a NULL pointer dereference flaw X509_issuer_and_serial_hash() were found, which could result in denial of service.

Additional details can be found in the upstream advisories https://www.openssl.org/news/secadv/20191206.txt and https://www.openssl.org/news/secadv/20210216.txt.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=947949
https://www.openssl.org/news/secadv/20191206.txt
https://www.openssl.org/news/secadv/20210216.txt
https://security-tracker.debian.org/tracker/source-package/openssl
https://packages.debian.org/source/buster/openssl
https://www.debian.org/security/2021/dsa-4855

Solution

Upgrade the openssl packages.

For the stable distribution (buster), these problems have been fixed in version 1.1.1d-0+deb10u5.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-1551
CVE	CVE-2021-23840
CVE	CVE-2021-23841
XREF	DSA:4855
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/02/19, Modified: 2024/01/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1d-0+deb10u5
```

146603 - Debian DSA-4857-1 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A buffer overflow vulnerability was discovered in the SPNEGO implementation affecting the GSSAPI security policy negotiation in BIND, a DNS server implementation, which could result in denial of service (daemon crash), or potentially the execution of arbitrary code.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=983004
https://security-tracker.debian.org/tracker/source-package/bind9
https://packages.debian.org/source/buster/bind9
https://www.debian.org/security/2021/dsa-4857

Solution

Upgrade the bind9 packages.

For the stable distribution (buster), this problem has been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u3.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-8625
XREF	DSA:4857

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u3
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u3
```

148170 - Debian DSA-4875-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A NULL pointer dereference was found in the signature_algorithms processing in OpenSSL, a Secure Sockets Layer toolkit, which could result in denial of service.

Additional details can be found in the upstream advisory:
https://www.openssl.org/news/secadv/20210325.txt

See Also

https://www.openssl.org/news/secadv/20210325.txt
https://security-tracker.debian.org/tracker/source-package/openssl
https://packages.debian.org/source/buster/openssl

https://www.debian.org/security/2021/dsa-4875

Solution

Upgrade the openssl packages.

For the stable distribution (buster), this problem has been fixed in version 1.1.1d-0+deb10u6.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3449
XREF	DSA:4875
XREF	IAVA:2021-A-0149-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/03/26, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1d-0+deb10u6
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1d-0+deb10u6
```

148277 - Debian DSA-4881-1 : curl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple vulnerabilities were discovered in cURL, an URL transfer library :

- CVE-2020-8169 Marek Szlagor reported that libcurl could be tricked into prepending a part of the password to the host name before it resolves it, potentially leaking the partial password over the network and to the DNS server(s).

- CVE-2020-8177 sn reported that curl could be tricked by a malicious server into overwriting a local file when using the -J (--remote-header-name) and -i (--include) options in the same command line.

- CVE-2020-8231 Marc Aldorasi reported that libcurl might use the wrong connection when an application using libcurl's multi API sets the option CURLOPT_CONNECT_ONLY, which could lead to information leaks.

- CVE-2020-8284 Varnavas Papaioannou reported that a malicious server could use the PASV response to trick curl into connecting back to an arbitrary IP address and port, potentially making curl extract information about services that are otherwise private and not disclosed.

- CVE-2020-8285 xnynx reported that libcurl could run out of stack space when using the FTP wildcard matching functionality (CURLOPT_CHUNK_BGN_FUNCTION).

- CVE-2020-8286 It was reported that libcurl didn't verify that an OCSP response actually matches the certificate it is intended to.

- CVE-2021-22876 Viktor Szakats reported that libcurl does not strip off user credentials from the URL when automatically populating the Referer HTTP request header field in outgoing HTTP requests.

- CVE-2021-22890 Mingtao Yang reported that, when using an HTTPS proxy and TLS 1.3, libcurl could confuse session tickets arriving from the HTTPS proxy as if they arrived from the remote server instead. This could allow an HTTPS proxy to trick libcurl into using the wrong session ticket for the host and thereby circumvent the server TLS certificate check.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=965280
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=965281
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=968831
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=977161
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=977162
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=977163
https://security-tracker.debian.org/tracker/CVE-2020-8169
https://security-tracker.debian.org/tracker/CVE-2020-8177
https://security-tracker.debian.org/tracker/CVE-2020-8231
https://security-tracker.debian.org/tracker/CVE-2020-8284
https://security-tracker.debian.org/tracker/CVE-2020-8285
https://security-tracker.debian.org/tracker/CVE-2020-8286
https://security-tracker.debian.org/tracker/CVE-2021-22876
https://security-tracker.debian.org/tracker/CVE-2021-22890
https://security-tracker.debian.org/tracker/source-package/curl
https://packages.debian.org/source/buster/curl
https://www.debian.org/security/2021/dsa-4881

Solution

Upgrade the curl packages.

For the stable distribution (buster), these problems have been fixed in version 7.64.0-4+deb10u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-8169
CVE	CVE-2020-8177
CVE	CVE-2020-8231
CVE	CVE-2020-8284
CVE	CVE-2020-8285
CVE	CVE-2020-8286
CVE	CVE-2021-22876
CVE	CVE-2021-22890
XREF	DSA:4881
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/04/01, Modified: 2024/01/16

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u2
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u2
```

149229 - Debian DSA-4909-1 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities were discovered in BIND, a DNS server implementation.

- CVE-2021-25214 Greg Kuechle discovered that a malformed incoming IXFR transfer could trigger an assertion failure in named, resulting in denial of service.

- CVE-2021-25215 Siva Kakarla discovered that named could crash when a DNAME record placed in the ANSWER section during DNAME chasing turned out to be the final answer to a client query.

- CVE-2021-25216 It was discovered that the SPNEGO implementation used by BIND is prone to a buffer overflow vulnerability. This update switches to use the SPNEGO implementation from the Kerberos libraries.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=987741
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=987742
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=987743
https://security-tracker.debian.org/tracker/CVE-2021-25214
https://security-tracker.debian.org/tracker/CVE-2021-25215
https://security-tracker.debian.org/tracker/CVE-2021-25216
https://security-tracker.debian.org/tracker/source-package/bind9
https://packages.debian.org/source/buster/bind9
https://www.debian.org/security/2021/dsa-4909

Solution

Upgrade the bind9 packages.

For the stable distribution (buster), these problems have been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u5.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-25214
CVE	CVE-2021-25215
CVE	CVE-2021-25216
XREF	DSA:4909

Plugin Information

Published: 2021/05/03, Modified: 2021/05/14

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
```

150905 - Debian DSA-4933-1 : nettle - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple vulnerabilities were discovered in nettle, a low level cryptographic library, which could result in denial of service (remote crash in RSA decryption via specially crafted ciphertext, crash on ECDSA signature verification) or incorrect verification of ECDSA signatures.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=985652
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=989631
https://security-tracker.debian.org/tracker/source-package/nettle
https://packages.debian.org/source/buster/nettle
https://www.debian.org/security/2021/dsa-4933

Solution

Upgrade the nettle packages.

For the stable distribution (buster), these problems have been fixed in version 3.4.1-1+deb10u1.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-20305
CVE	CVE-2021-3580
XREF	DSA:4933

Plugin Information

Published: 2021/06/21, Modified: 2023/12/21

Plugin Output

tcp/0

```
Remote package installed : libhogweed4_3.4.1-1
Should be : libhogweed4_3.4.1-1+deb10u1
Remote package installed : libnettle6_3.4.1-1
Should be : libnettle6_3.4.1-1+deb10u1
```

151833 - Debian DSA-4942-1 : systemd - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dsa-4942 advisory.

The Qualys Research Labs discovered that an attacker-controlled allocation using the alloca() function could result in memory corruption, allowing to crash systemd and hence the entire operating system.
Details can be found in the Qualys advisory at https://www.qualys.com/2021/07/20/cve-2021-33910/denial-of- service-systemd.txt For the stable distribution (buster), this problem has been fixed in version 241-7~deb10u8. We recommend that you upgrade your systemd packages. For the detailed security status of systemd please refer to its security tracker page at: https://security-tracker.debian.org/tracker/systemd

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/systemd
https://www.debian.org/security/2021/dsa-4942
https://security-tracker.debian.org/tracker/CVE-2021-33910
https://packages.debian.org/source/buster/systemd

Solution

Upgrade the systemd packages.

For the stable distribution (buster), this problem has been fixed in version 241-7~deb10u8.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2021-33910
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/20, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libpam-systemd_241-7~deb10u6
Should be : libpam-systemd_241-7~deb10u8
Remote package installed : libsystemd0_241-7~deb10u6
Should be : libsystemd0_241-7~deb10u8
Remote package installed : libudev1_241-7~deb10u6
Should be : libudev1_241-7~deb10u8
Remote package installed : systemd_241-7~deb10u6
Should be : systemd_241-7~deb10u8
Remote package installed : systemd-sysv_241-7~deb10u6
Should be : systemd-sysv_241-7~deb10u8
Remote package installed : udev_241-7~deb10u6
Should be : udev_241-7~deb10u8
```

152068 - Debian DSA-4944-1 : krb5 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dsa-4944 advisory.

- ec_verify in kdc/kdc_preauth_ec.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.4 and 1.19.x before 1.19.2 allows remote attackers to cause a NULL pointer dereference and daemon crash. This occurs because a return value is not properly managed in a certain situation. (CVE-2021-36222)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=991365
https://security-tracker.debian.org/tracker/source-package/krb5
https://www.debian.org/security/2021/dsa-4944
https://security-tracker.debian.org/tracker/CVE-2021-36222
https://packages.debian.org/source/buster/krb5

Solution

Upgrade the krb5 packages.

For the stable distribution (buster), this problem has been fixed in version 1.17-3+deb10u2.

Risk Factor

Medium

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)

CVSS v3.0 Temporal Score

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

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-2021-36222
XREF	IAVB:2021-B-0054-S

Plugin Information

Published: 2021/07/25, Modified: 2022/07/19

Plugin Output

tcp/0

```
Remote package installed : krb5-locales_1.17-3+deb10u1
Should be : krb5-locales_1.17-3+deb10u2
Remote package installed : libgssapi-krb5-2_1.17-3+deb10u1
Should be : libgssapi-krb5-2_1.17-3+deb10u2
Remote package installed : libk5crypto3_1.17-3+deb10u1
Should be : libk5crypto3_1.17-3+deb10u2
Remote package installed : libkrb5-3_1.17-3+deb10u1
Should be : libkrb5-3_1.17-3+deb10u2
Remote package installed : libkrb5support0_1.17-3+deb10u1
Should be : libkrb5support0_1.17-3+deb10u2
```

154707 - Debian DSA-4994-1 : bind9 - security update

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-4994 advisory.

- In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 ->
9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing. (CVE-2021-25219)

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

See Also

https://security-tracker.debian.org/tracker/source-package/bind9
https://www.debian.org/security/2021/dsa-4994
https://security-tracker.debian.org/tracker/CVE-2021-25219
https://packages.debian.org/source/buster/bind9
https://packages.debian.org/source/bullseye/bind9

Solution

Upgrade the bind9 packages.

For the stable distribution (bullseye), this problem has been fixed in version 1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-25219
XREF	IAVA:2021-A-0525-S

Plugin Information

Published: 2021/10/28, Modified: 2023/02/17

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u6
```

155709 - Debian DSA-5014-1 : icu - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dsa-5014 advisory.

- International Components for Unicode (ICU-20850) v66.1 was discovered to contain a use after free bug in the pkg_createWithAssemblyCode function in the file tools/pkgdata/pkgdata.cpp. (CVE-2020-21913)

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

See Also

https://security-tracker.debian.org/tracker/source-package/icu
https://www.debian.org/security/2021/dsa-5014

https://security-tracker.debian.org/tracker/CVE-2020-21913
https://packages.debian.org/source/buster/icu

Solution

Upgrade the icu packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-21913

Plugin Information

Published: 2021/11/29, Modified: 2023/11/22

Plugin Output

tcp/0

```
Remote package installed : libicu63_63.1-6+deb10u1
Should be : libicu63_63.1-6+deb10u2
```

158509 - Debian DSA-5087-1 : cyrus-sasl2 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5087 advisory.

- In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a SQL INSERT or UPDATE statement. (CVE-2022-24407)

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

See Also

https://security-tracker.debian.org/tracker/source-package/cyrus-sasl2
https://www.debian.org/security/2022/dsa-5087
https://security-tracker.debian.org/tracker/CVE-2022-24407
https://packages.debian.org/source/buster/cyrus-sasl2
https://packages.debian.org/source/bullseye/cyrus-sasl2

Solution

Upgrade the cyrus-sasl2 packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.1.27+dfsg-2.1+deb11u1.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-24407

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libsasl2-2_2.1.27+dfsg-1+deb10u1
Should be : libsasl2-2_2.1.27+dfsg-1+deb10u2
Remote package installed : libsasl2-modules_2.1.27+dfsg-1+deb10u1
Should be : libsasl2-modules_2.1.27+dfsg-1+deb10u2
Remote package installed : libsasl2-modules-db_2.1.27+dfsg-1+deb10u1
Should be : libsasl2-modules-db_2.1.27+dfsg-1+deb10u2
```

158979 - Debian DSA-5103-1 : openssl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5103 advisory.

Tavis Ormandy discovered that the BN_mod_sqrt() function of OpenSSL could be tricked into an infinite loop. This could result in denial of service via malformed certificates. Additional details can be found in the upstream advisory: https://www.openssl.org/news/secadv/20220315.txt In addition this update corrects a carry propagation bug specific to MIPS architectures. For the oldstable distribution (buster), this problem has been fixed in version 1.1.1d-0+deb10u8. For the stable distribution (bullseye), this problem has been fixed in version 1.1.1k-1+deb11u2. We recommend that you upgrade your openssl packages.
For the detailed security status of openssl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl

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

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=989604
https://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/security/2022/dsa-5103
https://security-tracker.debian.org/tracker/CVE-2021-4160
https://security-tracker.debian.org/tracker/CVE-2022-0778
https://packages.debian.org/source/buster/openssl
https://packages.debian.org/source/bullseye/openssl

Solution

Upgrade the openssl packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.1.1k-1+deb11u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-4160
CVE	CVE-2022-0778
XREF	IAVA:2021-A-0602-S

Plugin Information

Published: 2022/03/16, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1d-0+deb10u8
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1d-0+deb10u8
```

159109 - Debian DSA-5105-1 : bind9 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 / 11 host has packages installed that are affected by multiple vulnerabilities as referenced in the dsa-5105 advisory.

Two vulnerabilities were found in the BIND DNS server, which could result in denial of service or cache poisoning. For the oldstable distribution (buster), this problem has been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u7. For the stable distribution (bullseye), this problem has been fixed in version 1:9.16.27-1~deb11u1. We recommend that you upgrade your bind9 packages. For the detailed security status of bind9 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/bind9

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/bind9
https://www.debian.org/security/2022/dsa-5105
https://security-tracker.debian.org/tracker/CVE-2021-25220
https://security-tracker.debian.org/tracker/CVE-2022-0396
https://packages.debian.org/source/buster/bind9
https://packages.debian.org/source/bullseye/bind9

Solution

Upgrade the bind9 packages.

For the stable distribution (bullseye), this problem has been fixed in version 1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-25220
CVE	CVE-2022-0396
XREF	IAVA:2022-A-0122-S

Plugin Information

Published: 2022/03/21, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u7
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u2
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u7
```

159466 - Debian DSA-5111-1 : zlib - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5111 advisory.

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1008265
https://security-tracker.debian.org/tracker/source-package/zlib
https://www.debian.org/security/2022/dsa-5111
https://security-tracker.debian.org/tracker/CVE-2018-25032
https://packages.debian.org/source/buster/zlib
https://packages.debian.org/source/bullseye/zlib

Solution

Upgrade the zlib packages.

For the stable distribution (bullseye), this problem has been fixed in version 1

Risk Factor

Medium

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)

CVSS v3.0 Temporal Score

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

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

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

References

CVE CVE-2018-25032

Plugin Information

Published: 2022/04/01, Modified: 2023/11/03

Plugin Output

tcp/0

```
Remote package installed : zlib1g_1:1.2.11.dfsg-1
Should be : zlib1g_1:1.2.11.dfsg-1+deb10u1
```

161254 - Debian DSA-5137-1 : needrestart - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has a package installed that is affected by a vulnerability as referenced in the dsa-5137 advisory.

Jakub Wilk discovered a local privilege escalation in needrestart, a utility to check which daemons need to be restarted after library upgrades. Regular expressions to detect the Perl, Python, and Ruby interpreters are not anchored, allowing a local user to escalate privileges when needrestart tries to detect if interpreters are using old source files. For the oldstable distribution (buster), this problem has been fixed in version 3.4-5+deb10u1. For the stable distribution (bullseye), this problem has been fixed in version 3.5-4+deb11u1. We recommend that you upgrade your needrestart packages. For the detailed security status of needrestart please refer to its security tracker page at: https://security- tracker.debian.org/tracker/needrestart

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/needrestart
https://www.debian.org/security/2022/dsa-5137
https://security-tracker.debian.org/tracker/CVE-2022-30688
https://packages.debian.org/source/buster/needrestart
https://packages.debian.org/source/bullseye/needrestart

Solution

Upgrade the needrestart packages.

For the stable distribution (bullseye), this problem has been fixed in version 3.5-4+deb11u1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-30688

Plugin Information

Published: 2022/05/18, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : needrestart_3.4-5
Should be : needrestart_3.4-5+deb10u1
```

161434 - Debian DSA-5142-1 : libxml2 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5142 advisory.

- In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well. (CVE-2022-29824)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1010526
https://security-tracker.debian.org/tracker/source-package/libxml2
https://www.debian.org/security/2022/dsa-5142
https://security-tracker.debian.org/tracker/CVE-2022-29824
https://packages.debian.org/source/buster/libxml2
https://packages.debian.org/source/bullseye/libxml2

Solution

Upgrade the libxml2 packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.9.10+dfsg-6.7+deb11u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-29824

Plugin Information

Published: 2022/05/23, Modified: 2023/10/26

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-7+deb10u1
Should be : libxml2_2.9.4+dfsg1-7+deb10u4
```

161689 - Debian DSA-5150-1 : rsyslog - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5150 advisory.

- Rsyslog is a rocket-fast system for log processing. Modules for TCP syslog reception have a potential heap buffer overflow when octet-counted framing is used. This can result in a segfault or some other malfunction. As of our understanding, this vulnerability can not be used for remote code execution. But there may still be a slight chance for experts to do that. The bug occurs when the octet count is read.
While there is a check for the maximum number of octets, digits are written to a heap buffer even when the octet count is over the maximum, This can be used to overrun the memory buffer. However, once the sequence of digits stop, no additional characters can be added to the buffer. In our opinion, this makes remote exploits impossible or at least highly complex. Octet-counted framing is one of two potential framing modes. It is relatively uncommon, but enabled by default on receivers. Modules `imtcp`, `imptcp`, `imgssapi`, and `imhttp` are used for regular syslog message reception. It is best practice not to directly expose them to the public. When this practice is followed, the risk is considerably lower. Module `imdiag` is a diagnostics module primarily intended for testbench runs. We do not expect it to be present on any production installation. Octet-counted framing is not very common. Usually, it needs to be specifically enabled at senders. If users do not need it, they can turn it off for the most important modules. This will mitigate the vulnerability. (CVE-2022-24903)

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1010619
https://security-tracker.debian.org/tracker/source-package/rsyslog
https://www.debian.org/security/2022/dsa-5150
https://security-tracker.debian.org/tracker/CVE-2022-24903
https://packages.debian.org/source/buster/rsyslog
https://packages.debian.org/source/bullseye/rsyslog

Solution

Upgrade the rsyslog packages.

For the stable distribution (bullseye), this problem has been fixed in version 8.2102.0-2+deb11u1.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-24903

Plugin Information

Published: 2022/05/31, Modified: 2022/05/31

Plugin Output

tcp/0

```
Remote package installed : rsyslog_8.1901.0-1
Should be : rsyslog_8.1901.0-1+deb10u2
```

162701 - Debian DSA-5174-1 : gnupg2 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 / 11 host has packages installed that are affected by a vulnerability as referenced in the dsa-5174 advisory.

Demi Marie Obenour discovered a flaw in GnuPG, allowing for signature spoofing via arbitrary injection into the status line. An attacker who controls the secret part of any signing-capable key or subkey in the victim's keyring, can take advantage of this flaw to provide a correctly-formed signature that some software, including gpgme, will accept to have validity and signer fingerprint chosen from the attacker.
For the oldstable distribution (buster), this problem has been fixed in version 2.2.12-1+deb10u2. For the stable distribution (bullseye), this problem has been fixed in version 2.2.27-2+deb11u2. We recommend that you upgrade your gnupg2 packages. For the detailed security status of gnupg2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/gnupg2

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

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

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1014157
https://security-tracker.debian.org/tracker/source-package/gnupg2
https://www.debian.org/security/2022/dsa-5174
https://security-tracker.debian.org/tracker/CVE-2022-34903
https://packages.debian.org/source/buster/gnupg2
https://packages.debian.org/source/bullseye/gnupg2

Solution

Upgrade the gnupg2 packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.2.27-2+deb11u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-34903

Plugin Information

Published: 2022/07/04, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : gpgv_2.2.12-1+deb10u1
Should be : gpgv_2.2.12-1+deb10u2
```

164482 - Debian dla-3085 : curl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3085 advisory.

---------- Debian LTS Advisory DLA-3085-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany August 29, 2022 https://wiki.debian.org/LTS

Package : curl Version : 7.64.0-4+deb10u3 CVE ID : CVE-2021-22898 CVE-2021-22924 CVE-2021-22946 CVE-2021-22947 CVE-2022-22576 CVE-2022-27776 CVE-2022-27781 CVE-2022-27782 CVE-2022-32206 CVE-2022-32208 Debian Bug : 989228 991492 1010295 1010254 1010253 1010252

Multiple security vulnerabilities have been discovered in cURL, an URL transfer library. These flaws may allow remote attackers to obtain sensitive information, leak authentication or cookie header data or facilitate a denial of service attack.

For Debian 10 buster, these problems have been fixed in version 7.64.0-4+deb10u3.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2021-22898
https://security-tracker.debian.org/tracker/CVE-2021-22924
https://security-tracker.debian.org/tracker/CVE-2021-22946
https://security-tracker.debian.org/tracker/CVE-2021-22947
https://security-tracker.debian.org/tracker/CVE-2022-22576
https://security-tracker.debian.org/tracker/CVE-2022-27776
https://security-tracker.debian.org/tracker/CVE-2022-27781
https://security-tracker.debian.org/tracker/CVE-2022-27782
https://security-tracker.debian.org/tracker/CVE-2022-32206
https://security-tracker.debian.org/tracker/CVE-2022-32208
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2021-22898
CVE	CVE-2021-22924
CVE	CVE-2021-22946
CVE	CVE-2021-22947
CVE	CVE-2022-22576

CVE	CVE-2022-27776
CVE	CVE-2022-27781
CVE	CVE-2022-27782
CVE	CVE-2022-32206
CVE	CVE-2022-32208
XREF	IAVA:2022-A-0224-S
XREF	IAVA:2022-A-0255-S
XREF	CEA-ID:CEA-2022-0026

Plugin Information

Published: 2022/08/29, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u3
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u3
```

165983 - Debian dla-3142 : dbus - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3142 advisory.

- ---------- Debian LTS Advisory DLA-3142-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 10, 2022 https://wiki.debian.org/LTS
- ----------

Package : dbus Version : 1.12.24-0+deb10u1 CVE ID : CVE-2022-42010 CVE-2022-42011 CVE-2022-42012

Evgeny Vereshchagin discovered multiple vulnerabilities in D-Bus, a simple interprocess messaging system, which may result in denial of service by an authenticated user.

For Debian 10 buster, these problems have been fixed in version 1.12.24-0+deb10u1.

We recommend that you upgrade your dbus packages.

For the detailed security status of dbus please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/dbus

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/dbus
https://security-tracker.debian.org/tracker/CVE-2022-42010
https://security-tracker.debian.org/tracker/CVE-2022-42011
https://security-tracker.debian.org/tracker/CVE-2022-42012
https://packages.debian.org/source/buster/dbus

Solution

Upgrade the dbus packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-42010
CVE	CVE-2022-42011
CVE	CVE-2022-42012

Plugin Information

Published: 2022/10/10, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : dbus_1.12.20-0+deb10u1
Should be : dbus_1.12.24-0+deb10u1
Remote package installed : libdbus-1-3_1.12.20-0+deb10u1
Should be : libdbus-1-3_1.12.24-0+deb10u1
```

166092 - Debian dla-3145 : git - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3145 advisory.

---------- Debian LTS Advisory DLA-3145-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany October 11, 2022 https://wiki.debian.org/LTS

Package : git Version : 1:2.20.1-2+deb10u4 CVE ID : CVE-2021-21300 CVE-2021-40330 Debian Bug : 985120

Several security vulnerabilities have been discovered in Git, a fast, scalable, distributed revision control system, which may affect multi-user systems.

CVE-2021-21300

A specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS+ or APFS (i.e. the default file systems on Windows and macOS).

CVE-2021-40330

git_connect_git in connect.c allows a repository path to contain a newline character, which may result in unexpected cross-protocol requests, as demonstrated by the git://localhost:1234/%0d%0a%0d%0aGET%20/%20HTTP/1.1 substring.

For Debian 10 buster, these problems have been fixed in version 1:2.20.1-2+deb10u4.

We recommend that you upgrade your git packages.

For the detailed security status of git please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/git

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/git
https://security-tracker.debian.org/tracker/CVE-2021-21300
https://security-tracker.debian.org/tracker/CVE-2021-40330
https://packages.debian.org/source/buster/git

Solution

Upgrade the git packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-21300
CVE	CVE-2021-40330

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/10/13, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : git_1:2.20.1-2+deb10u3
Should be : git_1:2.20.1-2+deb10u4
Remote package installed : git-man_1:2.20.1-2+deb10u3
Should be : git-man_1:2.20.1-2+deb10u4
```

166004 - Debian dla-3146 : isc-dhcp-client - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3146 advisory.

- ---------- Debian LTS Advisory DLA-3146-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Utkarsh Gupta October 11, 2022 https://wiki.debian.org/LTS
- ----------

Package : isc-dhcp Version : 4.4.1-2+deb10u2 CVE ID : CVE-2022-2928 CVE-2022-2929 Debian Bug : 1021320

Several vulnerabilities have been discovered in the ISC DHCP client, relay and server.

CVE-2022-2928

It was discovered that the DHCP server does not correctly perform option reference counting when configured with allow leasequery;.
A remote attacker can take advantage of this flaw to cause a denial of service (daemon crash).

CVE-2022-2929

It was discovered that the DHCP server is prone to a memory leak flaw when handling contents of option 81 (fqdn) data received in a DHCP packet. A remote attacker can take advantage of this flaw to cause DHCP servers to consume resources, resulting in denial of service.

For Debian 10 buster, these problems have been fixed in version 4.4.1-2+deb10u2.

We recommend that you upgrade your isc-dhcp packages.

For the detailed security status of isc-dhcp please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/isc-dhcp

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/isc-dhcp
https://security-tracker.debian.org/tracker/CVE-2022-2928
https://security-tracker.debian.org/tracker/CVE-2022-2929
https://packages.debian.org/source/buster/isc-dhcp

Solution

Upgrade the isc-dhcp-client packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2928
CVE	CVE-2022-2929

Plugin Information

Published: 2022/10/11, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : isc-dhcp-client_4.4.1-2
Should be : isc-dhcp-client_4.4.1-2+deb10u2
Remote package installed : isc-dhcp-common_4.4.1-2
Should be : isc-dhcp-common_4.4.1-2+deb10u2
```

166708 - Debian dla-3167 : lib32ncurses-dev - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3167 advisory.

- ---------- Debian LTS Advisory DLA-3167-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz October 29, 2022 https://wiki.debian.org/LTS
- ----------

Package : ncurses Version : 6.1+20181013-2+deb10u3 CVE ID : CVE-2022-29458

An issue has been found in ncurses, a collection of shared libraries for terminal handling.
This issue is about an out-of-bounds read in convert_strings in the terminfo library.

For Debian 10 buster, this problem has been fixed in version 6.1+20181013-2+deb10u3.

We recommend that you upgrade your ncurses packages.

For the detailed security status of ncurses please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/ncurses

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LT

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/ncurses
https://security-tracker.debian.org/tracker/CVE-2022-29458
https://packages.debian.org/source/buster/ncurses

Solution

Upgrade the lib32ncurses-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-29458

Plugin Information

Published: 2022/10/30, Modified: 2025/01/22

Plugin Output

tcp/0

```
  Remote package installed : libncurses6_6.1+20181013-2+deb10u2
  Should be : libncurses6_6.1+20181013-2+deb10u3
  Remote package installed : libncursesw6_6.1+20181013-2+deb10u2
  Should be : libncursesw6_6.1+20181013-2+deb10u3
  Remote package installed : libtinfo6_6.1+20181013-2+deb10u2
  Should be : libtinfo6_6.1+20181013-2+deb10u3
  Remote package installed : ncurses-base_6.1+20181013-2+deb10u2
  Should be : ncurses-base_6.1+20181013-2+deb10u3
  Remote package installed : ncurses-bin_6.1+20181013-2+deb10u2
  Should be : ncurses-bin_6.1+20181013-2+deb10u3
  Remote package installed : ncurses-term_6.1+20181013-2+deb10u2
  Should be : ncurses-term_6.1+20181013-2+deb10u3
```

167256 - Debian dla-3182 : vim - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3182 advisory.

---------- Debian LTS Advisory DLA-3182-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany November 08, 2022 https://wiki.debian.org/LTS

Package : vim Version : 2:8.1.0875-5+deb10u3 CVE ID : CVE-2021-3927 CVE-2021-3928 CVE-2021-3974 CVE-2021-3984 CVE-2021-4019 CVE-2021-4069 CVE-2021-4192 CVE-2021-4193 CVE-2022-0213 CVE-2022-0261 CVE-2022-0319 CVE-2022-0351 CVE-2022-0359 CVE-2022-0361 CVE-2022-0368 CVE-2022-0408 CVE-2022-0413 CVE-2022-0417 CVE-2022-0443 CVE-2022-0554 CVE-2022-0572 CVE-2022-0685 CVE-2022-0714 CVE-2022-0729 CVE-2022-0943 CVE-2022-1154 CVE-2022-1616 CVE-2022-1720 CVE-2022-1851 CVE-2022-1898 CVE-2022-1968 CVE-2022-2285 CVE-2022-2304 CVE-2022-2598 CVE-2022-2946 CVE-2022-3099 CVE-2022-3134 CVE-2022-3234 CVE-2022-3324 CVE-2022-3705

Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and use-after-free may lead to a denial-of-service (application crash) or other unspecified impact.

For Debian 10 buster, these problems have been fixed in version 2:8.1.0875-5+deb10u3.

We recommend that you upgrade your vim packages.

For the detailed security status of vim please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/vim

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/vim
https://security-tracker.debian.org/tracker/CVE-2021-3927
https://security-tracker.debian.org/tracker/CVE-2021-3928
https://security-tracker.debian.org/tracker/CVE-2021-3974
https://security-tracker.debian.org/tracker/CVE-2021-3984
https://security-tracker.debian.org/tracker/CVE-2021-4019
https://security-tracker.debian.org/tracker/CVE-2021-4069
https://security-tracker.debian.org/tracker/CVE-2021-4192
https://security-tracker.debian.org/tracker/CVE-2021-4193
https://security-tracker.debian.org/tracker/CVE-2022-0213
https://security-tracker.debian.org/tracker/CVE-2022-0261
https://security-tracker.debian.org/tracker/CVE-2022-0319
https://security-tracker.debian.org/tracker/CVE-2022-0351
https://security-tracker.debian.org/tracker/CVE-2022-0359
https://security-tracker.debian.org/tracker/CVE-2022-0361
https://security-tracker.debian.org/tracker/CVE-2022-0368
https://security-tracker.debian.org/tracker/CVE-2022-0408
https://security-tracker.debian.org/tracker/CVE-2022-0413
https://security-tracker.debian.org/tracker/CVE-2022-0417
https://security-tracker.debian.org/tracker/CVE-2022-0443
https://security-tracker.debian.org/tracker/CVE-2022-0554
https://security-tracker.debian.org/tracker/CVE-2022-0572
https://security-tracker.debian.org/tracker/CVE-2022-0685
https://security-tracker.debian.org/tracker/CVE-2022-0714
https://security-tracker.debian.org/tracker/CVE-2022-0729
https://security-tracker.debian.org/tracker/CVE-2022-0943
https://security-tracker.debian.org/tracker/CVE-2022-1154
https://security-tracker.debian.org/tracker/CVE-2022-1616
https://security-tracker.debian.org/tracker/CVE-2022-1720
https://security-tracker.debian.org/tracker/CVE-2022-1851
https://security-tracker.debian.org/tracker/CVE-2022-1898
https://security-tracker.debian.org/tracker/CVE-2022-1968
https://security-tracker.debian.org/tracker/CVE-2022-2285
https://security-tracker.debian.org/tracker/CVE-2022-2304
https://security-tracker.debian.org/tracker/CVE-2022-2598
https://security-tracker.debian.org/tracker/CVE-2022-2946
https://security-tracker.debian.org/tracker/CVE-2022-3099
https://security-tracker.debian.org/tracker/CVE-2022-3134
https://security-tracker.debian.org/tracker/CVE-2022-3234

https://security-tracker.debian.org/tracker/CVE-2022-3324
https://security-tracker.debian.org/tracker/CVE-2022-3705
https://packages.debian.org/source/buster/vim

Solution

Upgrade the vim packages.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3927
CVE	CVE-2021-3928
CVE	CVE-2021-3974
CVE	CVE-2021-3984
CVE	CVE-2021-4019
CVE	CVE-2021-4069
CVE	CVE-2021-4192
CVE	CVE-2021-4193
CVE	CVE-2022-0213
CVE	CVE-2022-0261
CVE	CVE-2022-0319
CVE	CVE-2022-0351
CVE	CVE-2022-0359
CVE	CVE-2022-0361
CVE	CVE-2022-0368
CVE	CVE-2022-0408
CVE	CVE-2022-0413
CVE	CVE-2022-0417
CVE	CVE-2022-0443
CVE	CVE-2022-0554
CVE	CVE-2022-0572
CVE	CVE-2022-0685
CVE	CVE-2022-0714
CVE	CVE-2022-0729
CVE	CVE-2022-0943
CVE	CVE-2022-1154
CVE	CVE-2022-1616
CVE	CVE-2022-1720
CVE	CVE-2022-1851
CVE	CVE-2022-1898
CVE	CVE-2022-1968
CVE	CVE-2022-2285
CVE	CVE-2022-2304
CVE	CVE-2022-2598
CVE	CVE-2022-2946
CVE	CVE-2022-3099
CVE	CVE-2022-3134
CVE	CVE-2022-3234
CVE	CVE-2022-3324
CVE	CVE-2022-3705
XREF	IAVB:2022-B-0049-S
XREF	IAVB:2023-B-0016-S

Plugin Information

Published: 2022/11/10, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.1.0875-5
Should be : vim-common_2:8.1.0875-5+deb10u3
Remote package installed : vim-tiny_2:8.1.0875-5
Should be : vim-tiny_2:8.1.0875-5+deb10u3
Remote package installed : xxd_2:8.1.0875-5
Should be : xxd_2:8.1.0875-5+deb10u3
```

168740 - Debian dla-3239 : git - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3239 advisory.

- ---------- Debian LTS Advisory DLA-3239-2 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler December 14, 2022 https://wiki.debian.org/LTS
- ----------

Package : git Version : 1:2.20.1-2+deb10u6

In rare conditions, the previous git update released as DLA-3239-1 could generate a segmentation fault, which prevented its availability on armhf architecture. This update addresses this issue. For reference the original advisory text follows.

Multiple issues were found in Git, a distributed revision control system. An attacker may cause other local users into executing arbitrary commands, leak information from the local filesystem, and bypass restricted shell.

Note: Due to new security checks, access to repositories owned and accessed by different local users may now be rejected by Git; in case changing ownership is not practical, git displays a way to bypass these checks using the new 'safe.directory' configuration entry.

CVE-2022-24765

Git is not checking the ownership of directories in a local multi-user system when running commands specified in the local repository configuration. This allows the owner of the repository to cause arbitrary commands to be executed by other users who access the repository.

CVE-2022-29187

An unsuspecting user could still be affected by the issue reported in CVE-2022-24765, for example when navigating as root into a shared tmp directory that is owned by them, but where an attacker could create a git repository.

CVE-2022-39253

Exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine.

CVE-2022-39260

`git shell` improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine.

For Debian 10 buster, this problem has been fixed in version 1:2.20.1-2+deb10u6.

We recommend that you upgrade your git packages.

For the detailed security status of git please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/git

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/git
https://security-tracker.debian.org/tracker/CVE-2022-24765
https://security-tracker.debian.org/tracker/CVE-2022-29187
https://security-tracker.debian.org/tracker/CVE-2022-39253
https://security-tracker.debian.org/tracker/CVE-2022-39260
https://packages.debian.org/source/buster/git

Solution

Upgrade the git packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-24765
CVE	CVE-2022-29187
CVE	CVE-2022-39253
CVE	CVE-2022-39260

Plugin Information

Published: 2022/12/14, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : git_1:2.20.1-2+deb10u3
Should be : git_1:2.20.1-2+deb10u6
Remote package installed : git-man_1:2.20.1-2+deb10u3
Should be : git-man_1:2.20.1-2+deb10u6
```

170164 - Debian dla-3272 : sudo - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3272 advisory.

- ---------- Debian LTS Advisory DLA-3272-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz January 18, 2023 https://wiki.debian.org/LTS
- ----------

Package : sudo Version : 1.8.27-1+deb10u5 CVE ID : CVE-2023-22809

Matthieu Barjole and Victor Cutillas discovered that sudoedit in sudo, a program designed to provide limited super user privileges to specific users, does not properly handle '--' to separate the editor and arguments from files to edit. A local user permitted to edit certain files can take advantage of this flaw to edit a file not permitted by the security policy, resulting in privilege escalation.

More information can be found at:
https://www.sudo.ws/security/advisories/sudoedit_any/

For Debian 10 buster, this problem has been fixed in version 1.8.27-1+deb10u5.

We recommend that you upgrade your sudo packages.

For the detailed security status of sudo please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/sudo

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/sudo
https://security-tracker.debian.org/tracker/CVE-2023-22809
https://packages.debian.org/source/buster/sudo

Solution

Upgrade the sudo packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:H/RL:OF/RC:C)

References

CVE CVE-2023-22809

Exploitable With

Metasploit (true)

Plugin Information

Published: 2023/01/19, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.27-1+deb10u3
Should be : sudo_1.8.27-1+deb10u5
```

170757 - Debian dla-3288 : curl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3288 advisory.

---------- Debian LTS Advisory DLA-3288-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Roberto C. Snchez January 28, 2023 https://wiki.debian.org/LTS

Package : curl Version : 7.64.0-4+deb10u4 CVE ID : CVE-2022-27774 CVE-2022-32221 CVE-2022-35252 CVE-2022-43552 Debian Bug :

Several vulnerabilities were discovered in Curl, an easy-to-use client-side URL transfer library, which could result in denial of service or information disclosure.

This update also revises the fix for CVE-2022-27782 released in DLA-3085-1.

For Debian 10 buster, these problems have been fixed in version 7.64.0-4+deb10u4.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2022-27774
https://security-tracker.debian.org/tracker/CVE-2022-27782
https://security-tracker.debian.org/tracker/CVE-2022-32221
https://security-tracker.debian.org/tracker/CVE-2022-35252
https://security-tracker.debian.org/tracker/CVE-2022-43552
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

Risk Factor

Medium

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-27774
CVE	CVE-2022-27782
CVE	CVE-2022-32221
CVE	CVE-2022-35252
CVE	CVE-2022-43552
XREF	IAVA:2022-A-0451-S
XREF	IAVA:2022-A-0224-S
XREF	IAVA:2022-A-0350-S
XREF	IAVA:2023-A-0008-S

Plugin Information

Published: 2023/01/28, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
```

```
Should be : libcurl3-gnutls_7.64.0-4+deb10u4
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u4
```

171643 - Debian dla-3325 : libssl-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3325 advisory.

- ---------- Debian LTS Advisory DLA-3325-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort February 20, 2023 https://wiki.debian.org/LTS
- ----------

Package : openssl Version : 1.1.1n-0+deb10u4 CVE ID : CVE-2022-2097 CVE-2022-4304 CVE-2022-4450 CVE-2023-0215 CVE-2023-0286

Multiple vulnerabilities have been discovered in OpenSSL, a Secure Sockets Layer toolkit, which may result in incomplete encryption, side channel attacks, denial of service or information disclosure.

Additional details can be found in the upstream advisories at https://www.openssl.org/news/secadv/20220705.txt and https://www.openssl.org/news/secadv/20230207.txt

For Debian 10 buster, these problems have been fixed in version 1.1.1n-0+deb10u4.

We recommend that you upgrade your openssl packages.

For the detailed security status of openssl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openssl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://security-tracker.debian.org/tracker/CVE-2022-2097
https://security-tracker.debian.org/tracker/CVE-2022-4304
https://security-tracker.debian.org/tracker/CVE-2022-4450
https://security-tracker.debian.org/tracker/CVE-2023-0215
https://security-tracker.debian.org/tracker/CVE-2023-0286
https://packages.debian.org/source/buster/openssl

Solution

Upgrade the libssl-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-2097
CVE	CVE-2022-4304
CVE	CVE-2022-4450
CVE	CVE-2023-0215
CVE	CVE-2023-0286
XREF	IAVA:2022-A-0265-S
XREF	IAVA:2022-A-0518-S

Plugin Information

Published: 2023/02/20, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1n-0+deb10u4
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1n-0+deb10u4
```

171786 - Debian dla-3327 : libnss3 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3327 advisory.

---------- Debian LTS Advisory DLA-3327-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany February 20, 2023 https://wiki.debian.org/LTS

Package : nss Version : 2:3.42.1-1+deb10u6 CVE ID : CVE-2020-6829 CVE-2020-12400 CVE-2020-12401 CVE-2020-12403 CVE-2023-0767

Multiple security vulnerabilities have been discovered in nss, the Network Security Service libraries.

CVE-2020-6829

When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial information about the nonce used during signature generation. Given an electro-magnetic trace of a few signature generations, the private key could have been computed.

CVE-2020-12400

When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack.

CVE-2020-12401

During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data.

CVE-2020-12403

A flaw was found in the way CHACHA20-POLY1305 was implemented in NSS.
When using multi-part Chacha20, it could cause out-of-bounds reads.
This issue was fixed by explicitly disabling multi-part ChaCha20 (which was not functioning correctly) and strictly enforcing tag length.

CVE-2023-0767

Christian Holler discovered that incorrect handling of PKCS 12 Safe Bag attributes may result in execution of arbitrary code if a specially crafted PKCS 12 certificate bundle is processed.

For Debian 10 buster, these problems have been fixed in version 2:3.42.1-1+deb10u6.

We recommend that you upgrade your nss packages.

For the detailed security status of nss please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nss

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nss
https://security-tracker.debian.org/tracker/CVE-2020-12400
https://security-tracker.debian.org/tracker/CVE-2020-12401
https://security-tracker.debian.org/tracker/CVE-2020-12403
https://security-tracker.debian.org/tracker/CVE-2020-6829
https://security-tracker.debian.org/tracker/CVE-2023-0767
https://packages.debian.org/source/buster/nss

Solution

Upgrade the libnss3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-6829
CVE	CVE-2020-12400
CVE	CVE-2020-12401
CVE	CVE-2020-12403
CVE	CVE-2023-0767

Plugin Information

Published: 2023/02/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libnss3_2:3.42.1-1+deb10u3
Should be : libnss3_2:3.42.1-1+deb10u6
```

171753 - Debian dla-3332 : libaprutil1 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3332 advisory.

- ---------- Debian LTS Advisory DLA-3332-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk February 21, 2023 https://wiki.debian.org/LTS
- ----------

Package : apr-util Version : 1.6.1-4+deb10u1 CVE ID : CVE-2022-25147

An Integer Overflow or Wraparound vulnerability was fixed in apr_base64() in the Apache Portable Runtime Utility Library.

For Debian 10 buster, this problem has been fixed in version 1.6.1-4+deb10u1.

We recommend that you upgrade your apr-util packages.

For the detailed security status of apr-util please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/apr-util

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/apr-util
https://security-tracker.debian.org/tracker/CVE-2022-25147
https://packages.debian.org/source/buster/apr-util

Solution

Upgrade the libaprutil1 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-25147

Plugin Information

Published: 2023/02/21, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libaprutil1_1.6.1-4
Should be : libaprutil1_1.6.1-4+deb10u1
Remote package installed : libaprutil1-dbd-sqlite3_1.6.1-4
Should be : libaprutil1-dbd-sqlite3_1.6.1-4+deb10u1
Remote package installed : libaprutil1-ldap_1.6.1-4
Should be : libaprutil1-ldap_1.6.1-4+deb10u1
```

172449 - Debian dla-3351 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3351 advisory.

- ---------- Debian LTS Advisory DLA-3351-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Lee Garrett March 03, 2023 https://wiki.debian.org/LTS
- ----------

Package : apache2 Version : 2.4.38-3+deb10u9 CVE ID : CVE-2006-20001 CVE-2021-33193 CVE-2022-36760 CVE-2022-37436

Multiple security vulnerabilities have been discovered in Apache HTTP server.

CVE-2006-20001

A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

CVE-2021-33193

A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

CVE-2022-36760

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

CVE-2022-37436

A malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

For Debian 10 buster, these problems have been fixed in version 2.4.38-3+deb10u9.

We recommend that you upgrade your apache2 packages.

For the detailed security status of apache2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/apache2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://security-tracker.debian.org/tracker/CVE-2006-20001
https://security-tracker.debian.org/tracker/CVE-2021-33193
https://security-tracker.debian.org/tracker/CVE-2022-36760
https://security-tracker.debian.org/tracker/CVE-2022-37436
https://packages.debian.org/source/buster/apache2

Solution

Upgrade the apache2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2006-20001
CVE	CVE-2021-33193
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XREF	IAVA:2023-A-0047-S
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2023/03/10, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.38-3+deb10u9
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.38-3+deb10u9
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.38-3+deb10u9
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.38-3+deb10u9
```

172599 - Debian dla-3363 : libpcre2-16-0 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3363 advisory.

---------- Debian LTS Advisory DLA-3363-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin March 16, 2023 https://wiki.debian.org/LTS

Package : pcre2 Version : 10.32-5+deb10u1 CVE ID : CVE-2019-20454 CVE-2022-1586 CVE-2022-1587 Debian Bug : 1011954

Multiple out-of-bounds read vulnerabilities were found in pcre2, a Perl Compatible Regular Expression library, which could result in information disclosure or denial or service.

CVE-2019-20454

Out-of-bounds read when the pattern \X is JIT compiled and used to match specially crafted subjects in non-UTF mode.

CVE-2022-1586

Out-of-bounds read involving unicode property matching in JIT-compiled regular expressions. The issue occurs because the character was not fully read in case-less matching within JIT.

CVE-2022-1587

Out-of-bounds read affecting recursions in JIT-compiled regular expressions caused by duplicate data transfers.

This upload also fixes a subject buffer overread in JIT when UTF is disabled and \X or \R has a greater than 1 fixed quantifier. This issue was found by Yunho Kim.

For Debian 10 buster, these problems have been fixed in version 10.32-5+deb10u1.

We recommend that you upgrade your pcre2 packages.

For the detailed security status of pcre2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/pcre2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/pcre2
https://security-tracker.debian.org/tracker/CVE-2019-20454
https://security-tracker.debian.org/tracker/CVE-2022-1586
https://security-tracker.debian.org/tracker/CVE-2022-1587
https://packages.debian.org/source/buster/pcre2

Solution

Upgrade the libpcre2-16-0 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-20454
CVE	CVE-2022-1586
CVE	CVE-2022-1587

Plugin Information

Published: 2023/03/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpcre2-8-0_10.32-5
Should be : libpcre2-8-0_10.32-5+deb10u1
```

173457 - Debian dla-3369 : golang-github-opencontainers-runc-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3369 advisory.

- ---------- Debian LTS Advisory DLA-3369-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler March 27, 2023 https://wiki.debian.org/LTS
- ----------

Package : runc Version : 1.0.0~rc6+dfsg1-3+deb10u2 CVE ID : CVE-2019-16884 CVE-2019-19921 CVE-2021-30465 CVE-2022-29162 CVE-2023-27561 Debian Bug : 942026 988768

Multiple vulnerabilities were discovered in runc, the Open Container Project runtime, which is often used with virtualization environments such as Docker. Malicious Docker images or OCI bundles could breach isolation.

CVE-2019-16884

runc, as used in Docker and other products, allows AppArmor and SELinux restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.

CVE-2019-19921

runc has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)

CVE-2021-30465

runc allows a Container Filesystem Breakout via Directory Traversal. To exploit the vulnerability, an attacker must be able to create multiple containers with a fairly specific mount configuration. The problem occurs via a symlink-exchange attack that relies on a race condition.

CVE-2022-29162

`runc exec --cap` created processes with non-empty inheritable Linux process capabilities, creating an atypical Linux environment and enabling programs with inheritable file capabilities to elevate those capabilities to the permitted set during execve(2). This bug did not affect the container security sandbox as the inheritable set never contained more capabilities than were included in the container's bounding set.

CVE-2023-27561

CVE-2019-19921 was re-introduced by the fix for CVE-2021-30465.

For Debian 10 buster, this problem has been fixed in version 1.0.0~rc6+dfsg1-3+deb10u2.

We recommend that you upgrade your runc packages.

For the detailed security status of runc please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/runc

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/runc
https://security-tracker.debian.org/tracker/CVE-2019-16884
https://security-tracker.debian.org/tracker/CVE-2019-19921
https://security-tracker.debian.org/tracker/CVE-2021-30465
https://security-tracker.debian.org/tracker/CVE-2022-29162
https://security-tracker.debian.org/tracker/CVE-2023-27561
https://packages.debian.org/source/buster/runc

Solution

Upgrade the golang-github-opencontainers-runc-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-16884
CVE	CVE-2019-19921
CVE	CVE-2021-30465
CVE	CVE-2022-29162
CVE	CVE-2023-27561

Plugin Information

Published: 2023/03/28, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : runc_1.0.0~rc6+dfsg1-3
Should be : runc_1.0.0~rc6+dfsg1-3+deb10u2
```

173763 - Debian dla-3377 : libnss-myhostname - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3377 advisory.

- ---------- Debian LTS Advisory DLA-3377-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk March 31, 2023 https://wiki.debian.org/LTS
- ----------

Package : systemd Version : 241-7~deb10u9 CVE ID : CVE-2023-26604

Local privilege escalation for some sudo configurations has been fixed in systemd, the default init system in Debian.

For Debian 10 buster, this problem has been fixed in version 241-7~deb10u9.

We recommend that you upgrade your systemd packages.

For the detailed security status of systemd please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/systemd

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/systemd
https://security-tracker.debian.org/tracker/CVE-2023-26604
https://packages.debian.org/source/buster/systemd

Solution

Upgrade the libnss-myhostname packages.

For Debian 10 buster, this problem has been fixed in version 241-7~deb10u9.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-26604

Plugin Information

Published: 2023/04/02, Modified: 2025/01/22

Plugin Output

tcp/0

```
  Remote package installed : libpam-systemd_241-7~deb10u6
  Should be : libpam-systemd_241-7~deb10u9
  Remote package installed : libsystemd0_241-7~deb10u6
  Should be : libsystemd0_241-7~deb10u9
  Remote package installed : libudev1_241-7~deb10u6
  Should be : libudev1_241-7~deb10u9
  Remote package installed : systemd_241-7~deb10u6
  Should be : systemd_241-7~deb10u9
  Remote package installed : systemd-sysv_241-7~deb10u6
  Should be : systemd-sysv_241-7~deb10u9
  Remote package installed : udev_241-7~deb10u6
  Should be : udev_241-7~deb10u9
```

176664 - Debian dla-3445 : cpio - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3445 advisory.

- ---------- Debian LTS Advisory DLA-3445-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 04, 2023 https://wiki.debian.org/LTS
- ----------

Package : cpio Version : 2.12+dfsg-9+deb10u1 CVE ID : CVE-2019-14866 CVE-2021-38185 Debian Bug : 941412 992045

Two vulnerabilities were fixed in GNU cpio, a program to manage archives of files.

CVE-2019-14866

Improper validation of input files when generatingtar archives.

CVE-2021-38185

Arbitrary code via crafted pattern file.

For Debian 10 buster, these problems have been fixed in version 2.12+dfsg-9+deb10u1.

We recommend that you upgrade your cpio packages.

For the detailed security status of cpio please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/cpio

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/cpio
https://security-tracker.debian.org/tracker/CVE-2019-14866
https://security-tracker.debian.org/tracker/CVE-2021-38185
https://packages.debian.org/source/buster/cpio

Solution

Upgrade the cpio packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-14866
CVE	CVE-2021-38185

Plugin Information

Published: 2023/06/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : cpio_2.12+dfsg-9
Should be : cpio_2.12+dfsg-9+deb10u1
```

176985 - Debian dla-3449 : libssl-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3449 advisory.

- ---------- Debian LTS Advisory DLA-3449-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler June 08, 2023 https://wiki.debian.org/LTS
- ----------

Package : openssl Version : 1.1.1n-0+deb10u5 CVE ID : CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-2650 Debian Bug : 1034720

Multiple vulnerabilities have been discovered in OpenSSL, a Secure Sockets Layer toolkit.

CVE-2023-0464

David Benjamin reported a flaw related to the verification of X.509 certificate chains that include policy constraints, which may result in denial of service.

CVE-2023-0465

David Benjamin reported that invalid certificate policies in leaf certificates are silently ignored. A malicious CA could take advantage of this flaw to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether.

CVE-2023-0466

David Benjamin discovered that the implementation of the X509_VERIFY_PARAM_add0_policy() function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification (contrary to its documentation).

CVE-2023-2650

It was discovered that processing malformed ASN.1 object identifiers or data may result in denial of service.

For Debian 10 buster, these problems have been fixed in version 1.1.1n-0+deb10u5.

We recommend that you upgrade your openssl packages.

For the detailed security status of openssl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openssl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://security-tracker.debian.org/tracker/CVE-2023-0464
https://security-tracker.debian.org/tracker/CVE-2023-0465
https://security-tracker.debian.org/tracker/CVE-2023-0466
https://security-tracker.debian.org/tracker/CVE-2023-2650
https://packages.debian.org/source/buster/openssl

Solution

Upgrade the libssl-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-0464
CVE	CVE-2023-0465
CVE	CVE-2023-0466
CVE	CVE-2023-2650
XREF	IAVA:2023-A-0158-S

Plugin Information

Published: 2023/06/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1n-0+deb10u5
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1n-0+deb10u5
```

177513 - Debian dla-3461 : libfastjson-dev - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3461 advisory.

- ---------- Debian LTS Advisory DLA-3461-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz June 20, 2023 https://wiki.debian.org/LTS
- ----------

Package : libfastjson Version : 0.99.8-2+deb10u1 CVE ID : CVE-2020-12762

An issue has been found in libfastjson, a fast json library for C.
Due to missing checks, out-of-bounds write might happen when parsing large JSON files.

For Debian 10 buster, this problem has been fixed in version 0.99.8-2+deb10u1.

We recommend that you upgrade your libfastjson packages.

For the detailed security status of libfastjson please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libfastjson

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libfastjson
https://security-tracker.debian.org/tracker/CVE-2020-12762
https://packages.debian.org/source/buster/libfastjson

Solution

Upgrade the libfastjson-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-12762

Plugin Information

Published: 2023/06/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libfastjson4_0.99.8-2
Should be : libfastjson4_0.99.8-2+deb10u1
```

177792 - Debian dla-3474 : libnss-myhostname - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3474 advisory.

- ---------- Debian LTS Advisory DLA-3474-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 29, 2023 https://wiki.debian.org/LTS
- ----------

Package : systemd Version : 241-7~deb10u10 CVE ID : CVE-2022-3821 Debian Bug : 1021644

A buffer overrun in format_timespan() has been fixed in systemd, the default init system in Debian.

Additionally, fixes for getting property OnExternalPower via D-Bus and a memory leak on daemon-reload are also included.

For Debian 10 buster, this problem has been fixed in version 241-7~deb10u10.

We recommend that you upgrade your systemd packages.

For the detailed security status of systemd please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/systemd

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/systemd
https://security-tracker.debian.org/tracker/CVE-2022-3821
https://packages.debian.org/source/buster/systemd

Solution

Upgrade the libnss-myhostname packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-3821

Plugin Information

Published: 2023/06/30, Modified: 2025/01/22

Plugin Output

tcp/0

```
  Remote package installed : libpam-systemd_241-7~deb10u6
  Should be : libpam-systemd_241-7~deb10u10
  Remote package installed : libsystemd0_241-7~deb10u6
  Should be : libsystemd0_241-7~deb10u10
  Remote package installed : libudev1_241-7~deb10u6
  Should be : libudev1_241-7~deb10u10
  Remote package installed : systemd_241-7~deb10u6
  Should be : systemd_241-7~deb10u10
  Remote package installed : systemd-sysv_241-7~deb10u6
```

```
Should be : systemd-sysv_241-7~deb10u10
Remote package installed : udev_241-7~deb10u6
Should be : udev_241-7~deb10u10
```

179900 - Debian dla-3530 : libssl-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3530 advisory.

- ---------- Debian LTS Advisory DLA-3530-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Anton Gladky August 15, 2023 https://wiki.debian.org/LTS
- ----------

Package : openssl Version : 1.1.1n-0+deb10u6 CVE ID : CVE-2023-3446 CVE-2023-3817

Two vunerabilities were discovered in openssl, a Secure Sockets Layer toolkit:

CVE-2023-3446, CVE-2023-3817

Excessively long DH key or parameter checks can cause significant delays in applications using DH_check(), DH_check_ex(), or EVP_PKEY_param_check() functions, potentially leading to Denial of Service attacks when keys or parameters are obtained from untrusted sources.

For Debian 10 buster, these problems have been fixed in version 1.1.1n-0+deb10u6.

We recommend that you upgrade your openssl packages.

For the detailed security status of openssl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://security-tracker.debian.org/tracker/CVE-2023-3446
https://security-tracker.debian.org/tracker/CVE-2023-3817
https://packages.debian.org/source/buster/openssl

Solution

Upgrade the libssl-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2023-3446
CVE	CVE-2023-3817
XREF	IAVA:2023-A-0398-S

Plugin Information

Published: 2023/08/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.1d-0+deb10u4
Should be : libssl1.1_1.1.1n-0+deb10u6
Remote package installed : openssl_1.1.1d-0+deb10u5
Should be : openssl_1.1.1n-0+deb10u6
```

181187 - Debian dla-3559 : libssh2-1 - security update

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3559 advisory.

---------- Debian LTS Advisory DLA-3559-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin September 08, 2023 https://wiki.debian.org/LTS

Package : libssh2 Version : 1.8.0-2.1+deb10u1 CVE ID : CVE-2019-13115 CVE-2019-17498 CVE-2020-22218 Debian Bug : 932329 943562

Vulnerabilities were found in libssh2, a client-side C library implementing the SSH2 protocol, which could lead to denial of service or remote information disclosure.

CVE-2019-13115

Kevin Backhouse discovered an integer overflow vulnerability in kex.c's kex_method_diffie_hellman_group_exchange_sha256_key_exchange() function, which could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises an SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.

CVE-2019-17498

Kevin Backhouse discovered that the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, thereby enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A malicious SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.

CVE-2020-22218

An issue was discovered in function _libssh2_packet_add(), which could allow attackers to access out of bounds memory.

For Debian 10 buster, these problems have been fixed in version 1.8.0-2.1+deb10u1.

We recommend that you upgrade your libssh2 packages.

For the detailed security status of libssh2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libssh2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libssh2
https://security-tracker.debian.org/tracker/CVE-2019-13115
https://security-tracker.debian.org/tracker/CVE-2019-17498
https://security-tracker.debian.org/tracker/CVE-2020-22218
https://packages.debian.org/source/buster/libssh2

Solution

Upgrade the libssh2-1 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-13115
CVE	CVE-2019-17498
CVE	CVE-2020-22218

Plugin Information

Published: 2023/09/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libssh2-1_1.8.0-2.1
Should be : libssh2-1_1.8.0-2.1+deb10u1
```

181697 - Debian dla-3575 : idle-python2.7 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3575 advisory.

---------- Debian LTS Advisory DLA-3575-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Helmut Grohne September 20, 2023 https://wiki.debian.org/LTS

Package : python2.7 Version : 2.7.16-2+deb10u3 CVE ID : CVE-2021-23336 CVE-2022-0391 CVE-2022-48560 CVE-2022-48565 CVE-2022-48566 CVE-2023-24329 CVE-2023-40217

This update fixes multiple vulnerabilities concerning the urlparse module as well as vulnerabilities concerning the heapq, hmac, plistlib and ssl modules.

CVE-2021-23336

Python was vulnerable to Web Cache Poisoning via urlparse.parse_qsl and urlparse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.

CVE-2022-0391

The urlparse module helps break Uniform Resource Locator (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like '\r' and '

' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks.

CVE-2022-48560

A use-after-free exists in Python via heappushpop in heapq.

CVE-2022-48565

An XML External Entity (XXE) issue was discovered in Python. The plistlib module no longer accepts entity declarations in XML plist files to avoid XML vulnerabilities.

CVE-2022-48566

An issue was discovered in compare_digest in Lib/hmac.py in Python.
Constant-time-defeating optimisations were possible in the accumulator variable in hmac.compare_digest.

CVE-2023-24329

An issue in the urlparse component of Python allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.

CVE-2023-40217

The issue primarily affects servers written in Python (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as not connected and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)

For Debian 10 buster, these problems have been fixed in version 2.7.16-2+deb10u3.

We recommend that you upgrade your python2.7 packages.

For the detailed security status of python2.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python2.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python2.7
https://security-tracker.debian.org/tracker/CVE-2021-23336
https://security-tracker.debian.org/tracker/CVE-2022-0391
https://security-tracker.debian.org/tracker/CVE-2022-48560
https://security-tracker.debian.org/tracker/CVE-2022-48565
https://security-tracker.debian.org/tracker/CVE-2022-48566
https://security-tracker.debian.org/tracker/CVE-2023-24329
https://security-tracker.debian.org/tracker/CVE-2023-40217
https://packages.debian.org/source/buster/python2.7

Solution

Upgrade the idle-python2.7 packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-23336
CVE	CVE-2022-0391
CVE	CVE-2022-48560
CVE	CVE-2022-48565
CVE	CVE-2022-48566
CVE	CVE-2023-24329
CVE	CVE-2023-40217

Plugin Information

Published: 2023/09/20, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.16-2+deb10u1
Should be : libpython2.7-minimal_2.7.16-2+deb10u3
Remote package installed : libpython2.7-stdlib_2.7.16-2+deb10u1
Should be : libpython2.7-stdlib_2.7.16-2+deb10u3
Remote package installed : python2.7_2.7.16-2+deb10u1
Should be : python2.7_2.7.16-2+deb10u3
Remote package installed : python2.7-minimal_2.7.16-2+deb10u1
Should be : python2.7-minimal_2.7.16-2+deb10u3
```

181835 - Debian dla-3579 : elfutils - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3579 advisory.

- ---------- Debian LTS Advisory DLA-3579-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz September 23, 2023 https://wiki.debian.org/LTS
- ----------

Package : elfutils Version : 0.176-1.1+deb10u1 CVE ID : CVE-2020-21047

An issue has been found in elfutils, a collection of utilities to handle ELF objects.
Due to missing bound checks and reachable asserts, an attacker can use crafted elf files to trigger application crashes that result in denial-of-services.

For Debian 10 buster, this problem has been fixed in version 0.176-1.1+deb10u1.

We recommend that you upgrade your elfutils packages.

For the detailed security status of elfutils please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/elfutils

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/elfutils
https://security-tracker.debian.org/tracker/CVE-2020-21047
https://packages.debian.org/source/buster/elfutils

Solution

Upgrade the elfutils packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-21047

Plugin Information

Published: 2023/09/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libelf1_0.176-1.1
Should be : libelf1_0.176-1.1+deb10u1
```

182584 - Debian dla-3602 : libx11-6 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3602 advisory.

- ---------- Debian LTS Advisory DLA-3602-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 05, 2023 https://wiki.debian.org/LTS
- ----------

Package : libx11 Version : 2:1.6.7-1+deb10u4 CVE ID : CVE-2023-43785 CVE-2023-43786 CVE-2023-43787

Several vulnerabilities were found in libx11, the X11 client-side library.

CVE-2023-43785

Gregory James Duck discovered an out of bounds memory access in
_XkbReadKeySyms, which could result in denial of service.

CVE-2023-43786

Yair Mizrahi found an infinite recursion in PutSubImage when parsing a crafted file, which would result in stack exhaustion and denial of service.

CVE-2023-43787

Yair Mizrahi discovered an integer overflow in XCreateImage when parsing crafted input, which would result in a small buffer allocation leading into a buffer overflow. This could result in denial of service or potentially in arbitrary code execution.

For Debian 10 buster, these problems have been fixed in version 2:1.6.7-1+deb10u4.

We recommend that you upgrade your libx11 packages.

For the detailed security status of libx11 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libx11

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:

https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/libx11
https://security-tracker.debian.org/tracker/CVE-2023-43785
https://security-tracker.debian.org/tracker/CVE-2023-43786
https://security-tracker.debian.org/tracker/CVE-2023-43787
https://packages.debian.org/source/buster/libx11

Solution

Upgrade the libx11-6 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-43785
CVE	CVE-2023-43786
CVE	CVE-2023-43787

Plugin Information

Published: 2023/10/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.7-1+deb10u1
Should be : libx11-6_2:1.6.7-1+deb10u4
Remote package installed : libx11-data_2:1.6.7-1+deb10u1
Should be : libx11-data_2:1.6.7-1+deb10u4
```

182650 - Debian dla-3605 : grub-common - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3605 advisory.

- ---------- Debian LTS Advisory DLA-3605-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Utkarsh Gupta October 06, 2023 https://wiki.debian.org/LTS
- ----------

Package : grub2 Version : 2.06-3~deb10u4 CVE ID : CVE-2023-4692 CVE-2023-4693

A couple of security issues were reported in grub2 package, which is GRand Unified Bootloader v2, that could cause out-of-bounds write and heap-based buffer overflow.

For Debian 10 buster, these problems have been fixed in version 2.06-3~deb10u4.

We recommend that you upgrade your grub2 packages.

For the detailed security status of grub2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/grub2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/grub2
https://security-tracker.debian.org/tracker/CVE-2023-4692
https://security-tracker.debian.org/tracker/CVE-2023-4693
https://packages.debian.org/source/buster/grub2

Solution

Upgrade the grub-common packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-4692
CVE	CVE-2023-4693

Plugin Information

Published: 2023/10/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : grub-common_2.02+dfsg1-20+deb10u4
Should be : grub-common_2.06-3~deb10u4
Remote package installed : grub-pc_2.02+dfsg1-20+deb10u4
Should be : grub-pc_2.06-3~deb10u4
Remote package installed : grub-pc-bin_2.02+dfsg1-20+deb10u4
Should be : grub-pc-bin_2.06-3~deb10u4
Remote package installed : grub2-common_2.02+dfsg1-20+deb10u4
Should be : grub2-common_2.06-3~deb10u4
```

182933 - Debian dla-3613 : curl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3613 advisory.

- ---------- Debian LTS Advisory DLA-3613-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 11, 2023 https://wiki.debian.org/LTS

- --

Package : curl Version : 7.64.0-4+deb10u7 CVE ID : CVE-2023-28321 CVE-2023-38546

Two security issues were found in Curl, an easy-to-use client-side URL transfer library and command line tool.

CVE-2023-28321

Hiroki Kurosawa found that curl could mismatch hostnames with wildcards when using its own name matching function.

CVE-2023-38546

It was discovered that under some circumstances libcurl was susceptible to cookie injection.

For Debian 10 buster, these problems have been fixed in version 7.64.0-4+deb10u7.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2023-28321
https://security-tracker.debian.org/tracker/CVE-2023-38546
https://packages.debian.org/source/buster/curl

Solution

Upgrade the curl packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-28321
CVE	CVE-2023-38546
XREF	IAVA:2023-A-0259-S
XREF	CEA-ID:CEA-2023-0052
XREF	IAVA:2023-A-0531-S

Plugin Information

Published: 2023/10/11, Modified: 2025/01/23

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u7
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u7
```

183195 - Debian dla-3621 : libnghttp2-14 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3621 advisory.

---------- Debian LTS Advisory DLA-3621-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton October 16, 2023 https://wiki.debian.org/LTS

Package : nghttp2 Version : 1.36.0-2+deb10u2 CVE ID : CVE-2020-11080 CVE-2023-44487 Debian Bug : 962145 1053769

Multiple vulnerabilities were discovered in nghttp2, an implementation of the HTTP/2 protocol.

CVE-2020-11080

A denial-of-service could be caused by a large HTTP/2 SETTINGS frame payload.

CVE-2023-44487

A denial-of-service could be caused by resetting many HTTP/2 streams quickly. This has been observed in the wild since August.

For Debian 10 buster, these problems have been fixed in version 1.36.0-2+deb10u2.

We recommend that you upgrade your nghttp2 packages.

For the detailed security status of nghttp2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nghttp2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nghttp2
https://security-tracker.debian.org/tracker/CVE-2020-11080
https://security-tracker.debian.org/tracker/CVE-2023-44487
https://packages.debian.org/source/buster/nghttp2

Solution

Upgrade the libnghttp2-14 packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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)

CVSS v3.0 Temporal Score

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

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

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

STIG Severity

I

References

CVE	CVE-2020-11080
CVE	CVE-2023-44487
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2024-0004
XREF	IAVB:2023-B-0083-S

Plugin Information

Published: 2023/10/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libnghttp2-14_1.36.0-2+deb10u1
Should be : libnghttp2-14_1.36.0-2+deb10u2
```

183680 - Debian dla-3626 : krb5-admin-server - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3626 advisory.

- ---------- Debian LTS Advisory DLA-3626-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk October 22, 2023 https://wiki.debian.org/LTS
- ----------

Package : krb5 Version : 1.17-3+deb10u6 CVE ID : CVE-2023-36054 Debian Bug : 1043431

Potential freeing of an uninitialized pointer in kadm_rpc_xdr.c was fixed in krb5, the MIT implementation of the Kerberos network authentication protocol.

For Debian 10 buster, this problem has been fixed in version 1.17-3+deb10u6.

We recommend that you upgrade your krb5 packages.

For the detailed security status of krb5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/krb5

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/krb5
https://security-tracker.debian.org/tracker/CVE-2023-36054
https://packages.debian.org/source/buster/krb5

Solution

Upgrade the krb5-admin-server packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-36054

Plugin Information

Published: 2023/10/23, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : krb5-locales_1.17-3+deb10u1
Should be : krb5-locales_1.17-3+deb10u6
Remote package installed : libgssapi-krb5-2_1.17-3+deb10u1
Should be : libgssapi-krb5-2_1.17-3+deb10u6
Remote package installed : libk5crypto3_1.17-3+deb10u1
Should be : libk5crypto3_1.17-3+deb10u6
Remote package installed : libkrb5-3_1.17-3+deb10u1
Should be : libkrb5-3_1.17-3+deb10u6
Remote package installed : libkrb5support0_1.17-3+deb10u1
Should be : libkrb5support0_1.17-3+deb10u6
```

183747 - Debian dla-3628 : dbus - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3628 advisory.

- ---------- Debian LTS Advisory DLA-3628-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 23, 2023 https://wiki.debian.org/LTS
- ----------

Package : dbus Version : 1.12.28-0+deb10u1 CVE ID : CVE-2023-34969

It was found that D-Bus, a simple interprocess messaging system, was susceptible to a denial of service vulnerability if a monitor was being run.

For Debian 10 buster, this problem has been fixed in version 1.12.28-0+deb10u1.

We recommend that you upgrade your dbus packages.

For the detailed security status of dbus please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/dbus

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/dbus

https://security-tracker.debian.org/tracker/CVE-2023-34969
https://packages.debian.org/source/buster/dbus

Solution

Upgrade the dbus packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-34969

Plugin Information

Published: 2023/10/23, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : dbus_1.12.20-0+deb10u1
Should be : dbus_1.12.28-0+deb10u1
Remote package installed : libdbus-1-3_1.12.20-0+deb10u1
Should be : libdbus-1-3_1.12.28-0+deb10u1
```

183996 - Debian dla-3634 : libnss3 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3634 advisory.

---------- Debian LTS Advisory DLA-3634-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton October 28, 2023 https://wiki.debian.org/LTS

Package : nss Version : 2:3.42.1-1+deb10u7 CVE ID : CVE-2020-25648 CVE-2023-4421

Multiple vulnerabilities were found in nss, a set of libraries designed to support cross-platform development of security-enabled client and server applications.

CVE-2020-25648

A flaw was discovered in how NSS handles CipherChangeSpec messages in TLS 1.3. It could allow an attacker to send multiple CCS messages to servers compiled against NSS, causing denial-of-service.

CVE-2023-4421

A fuzzing project discovered vulnerabilities to Bleichenbacher timing attacks in NSS's facilities for RSA cryptography.

For Debian 10 buster, these problems have been fixed in version 2:3.42.1-1+deb10u7.

We recommend that you upgrade your nss packages.

For the detailed security status of nss please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nss

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nss
https://security-tracker.debian.org/tracker/CVE-2020-25648
https://security-tracker.debian.org/tracker/CVE-2023-4421
https://packages.debian.org/source/buster/nss

Solution

Upgrade the libnss3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

References

CVE	CVE-2020-25648
CVE	CVE-2023-4421

Plugin Information

Published: 2023/10/28, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libnss3_2:3.42.1-1+deb10u3
Should be : libnss3_2:3.42.1-1+deb10u7
```

186205 - Debian dla-3660 : gnutls-bin - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3660 advisory.

---------- Debian LTS Advisory DLA-3660-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany November 22, 2023 https://wiki.debian.org/LTS

Package : gnutls28 Version : 3.6.7-4+deb10u11 CVE ID : CVE-2023-5981 Debian Bug : 1056188

A vulnerability was found in GnuTLS, a secure communications library, which may facilitate a timing attack to compromise a cryptographic system. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. Only TLS ciphertext processing is affected.

For Debian 10 buster, this problem has been fixed in version 3.6.7-4+deb10u11.

We recommend that you upgrade your gnutls28 packages.

For the detailed security status of gnutls28 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/gnutls28

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/gnutls28
https://security-tracker.debian.org/tracker/CVE-2023-5981
https://packages.debian.org/source/buster/gnutls28

Solution

Upgrade the gnutls-bin packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-5981

Plugin Information

Published: 2023/11/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libgnutls30_3.6.7-4+deb10u6
Should be : libgnutls30_3.6.7-4+deb10u11
```

186526 - Debian dla-3682 : lib32ncurses-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3682 advisory.

---------- Debian LTS Advisory DLA-3682-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin December 03, 2023 https://wiki.debian.org/LTS

Package : ncurses Version : 6.1+20181013-2+deb10u5 CVE ID : CVE-2021-39537 CVE-2023-29491 Debian Bug : 1034372

Issues were found in ncurses, a collection of shared libraries for terminal handling, which could lead to denial of service.

CVE-2021-39537

It has been discovered that the tic(1) utility is susceptible to a heap overflow on crafted input due to improper bounds checking.

CVE-2023-29491

Jonathan Bar Or, Michael Pearse and Emanuele Cozzi have discovered that when ncurses is used by a setuid application, a local user can trigger security-relevant memory corruption via malformed data in a terminfo database file found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variables.

In order to mitigate this issue, ncurses now further restricts programs running with elevated privileges (setuid/setgid programs).
Programs run by the superuser remain able to load custom terminfo entries.

This change aligns ncurses' behavior in buster-security with that of Debian Bullseye's latest point release (6.2+20201114-2+deb11u2).

For Debian 10 buster, these problems have been fixed in version 6.1+20181013-2+deb10u5.

We recommend that you upgrade your ncurses packages.

For the detailed security status of ncurses please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/ncurses

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/ncurses
https://security-tracker.debian.org/tracker/CVE-2021-39537
https://security-tracker.debian.org/tracker/CVE-2023-29491
https://packages.debian.org/source/buster/ncurses

Solution

Upgrade the lib32ncurses-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-39537
CVE	CVE-2023-29491

Plugin Information

Published: 2023/12/03, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libncurses6_6.1+20181013-2+deb10u2
Should be : libncurses6_6.1+20181013-2+deb10u5
Remote package installed : libncursesw6_6.1+20181013-2+deb10u2
Should be : libncursesw6_6.1+20181013-2+deb10u5
Remote package installed : libtinfo6_6.1+20181013-2+deb10u2
Should be : libtinfo6_6.1+20181013-2+deb10u5
Remote package installed : ncurses-base_6.1+20181013-2+deb10u2
Should be : ncurses-base_6.1+20181013-2+deb10u5
Remote package installed : ncurses-bin_6.1+20181013-2+deb10u2
Should be : ncurses-bin_6.1+20181013-2+deb10u5
Remote package installed : ncurses-term_6.1+20181013-2+deb10u2
Should be : ncurses-term_6.1+20181013-2+deb10u5
```

187271 - Debian dla-3692 : curl - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3692 advisory.

- ---------- Debian LTS Advisory DLA-3692-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk December 19, 2023 https://wiki.debian.org/LTS
- ----------

Package : curl Version : 7.64.0-4+deb10u8 CVE ID : CVE-2023-28322 CVE-2023-46218 Debian Bug : 926148 1036239 1057646

Two security issues were found in Curl, an easy-to-use client-side URL transfer library and command line tool.

Additionally, the command line tool does now:
- - display the Debian revision in curl --version, and
- - does no longer output verbose Expire in messsages with curl -v

CVE-2023-28322

POST-after-PUT confusion.

CVE-2023-46218

Cookie mixed case PSL bypass.

For Debian 10 buster, these problems have been fixed in version 7.64.0-4+deb10u8.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://packages.debian.org/source/buster/curl
https://security-tracker.debian.org/tracker/source-package/curl
https://security-tracker.debian.org/tracker/CVE-2023-28322
https://security-tracker.debian.org/tracker/CVE-2023-46218

Solution

Upgrade the curl packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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 v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-28322
CVE	CVE-2023-46218
XREF	IAVA:2023-A-0259-S
XREF	IAVA:2023-A-0674-S

Plugin Information

Published: 2023/12/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.64.0-4+deb10u1
Should be : libcurl3-gnutls_7.64.0-4+deb10u8
Remote package installed : libcurl4_7.64.0-4+deb10u1
Should be : libcurl4_7.64.0-4+deb10u8
```

214473 - Debian dla-3694 : openssh-client - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3694 advisory.

---------- Debian LTS Advisory DLA-3694-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Santiago Ruano Rincn December 25, 2023 https://wiki.debian.org/LTS

Package : openssh Version : 1:7.9p1-10+deb10u4 CVE ID : CVE-2021-41617 CVE-2023-48795 CVE-2023-51385 Debian Bug : 995130

Several vulnerabilities have been discovered in OpenSSH, an implementation of the SSH protocol suite.

CVE-2021-41617

It was discovered that sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with.

CVE-2023-48795

Fabian Baeumer, Marcus Brinkmann and Joerg Schwenk discovered that the SSH protocol is prone to a prefix truncation attack, known as the Terrapin attack. This attack allows a MITM attacker to effect a limited break of the integrity of the early encrypted SSH transport protocol by sending extra messages prior to the commencement of encryption, and deleting an equal number of consecutive messages immediately after encryption starts.

Details can be found at https://terrapin-attack.com/

CVE-2023-51385

It was discovered that if an invalid user or hostname that contained shell metacharacters was passed to ssh, and a ProxyCommand, LocalCommand directive or match exec predicate referenced the user or hostname via expansion tokens, then an attacker who could supply arbitrary user/hostnames to ssh could potentially

perform command injection. The situation could arise in case of git repositories with submodules, where the repository could contain a submodule with shell characters in its user or hostname.

For Debian 10 buster, these problems have been fixed in version 1:7.9p1-10+deb10u4.

We recommend that you upgrade your openssh packages.

For the detailed security status of openssh please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssh

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/openssh
https://security-tracker.debian.org/tracker/CVE-2021-41617
https://security-tracker.debian.org/tracker/CVE-2023-48795
https://security-tracker.debian.org/tracker/CVE-2023-51385
https://packages.debian.org/source/buster/openssh

Solution

Upgrade the openssh-client packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-41617
CVE	CVE-2023-48795
CVE	CVE-2023-51385
XREF	IAVA:2021-A-0474-S
XREF	IAVA:2023-A-0701-S
XREF	IAVA:2023-A-0703

Plugin Information

Published: 2025/01/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : openssh-client_1:7.9p1-10+deb10u2
Should be : openssh-client_1:7.9p1-10+deb10u4
Remote package installed : openssh-server_1:7.9p1-10+deb10u2
Should be : openssh-server_1:7.9p1-10+deb10u4
```

```
Remote package installed : openssh-sftp-server_1:7.9p1-10+deb10u2
Should be : openssh-sftp-server_1:7.9p1-10+deb10u4
```

190686 - Debian dla-3735 : golang-github-opencontainers-runc-dev - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3735 advisory.

---------- Debian LTS Advisory DLA-3735-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Daniel Leidert February 19, 2024 https://wiki.debian.org/LTS

Package : runc Version : 1.0.0~rc6+dfsg1-3+deb10u3 CVE ID : CVE-2021-43784 CVE-2024-21626 Debian Bug :

runc is a command line client for running applications packaged according to the Open Container Format (OCF) and is a compliant implementation of the Open Container Project specification.

CVE-2021-43784

A flaw has been detected that may lead to a possible length field overflow, allowing user-controlled data to be parsed as control characters.

CVE-2024-21626

A flaw has been detected which allows several container breakouts due to internally leaked file descriptors. The patch includes fixes and hardening measurements against these types of issues/attacks.

For Debian 10 buster, these problems have been fixed in version 1.0.0~rc6+dfsg1-3+deb10u3.

We recommend that you upgrade your runc packages.

For the detailed security status of runc please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/runc

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Attachment:
signature.asc Description: This is a digitally signed message part

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/runc
https://security-tracker.debian.org/tracker/CVE-2021-43784
https://security-tracker.debian.org/tracker/CVE-2024-21626
https://packages.debian.org/source/buster/runc

Solution

Upgrade the golang-github-opencontainers-runc-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-43784
CVE	CVE-2024-21626
XREF	IAVA:2024-A-0071

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/02/19, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : runc_1.0.0~rc6+dfsg1-3
Should be : runc_1.0.0~rc6+dfsg1-3+deb10u3
```

191776 - Debian dla-3755 : tar - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3755 advisory.

- ---------- Debian LTS Advisory DLA-3755-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk March 09, 2024 https://wiki.debian.org/LTS
- ----------

Package : tar Version : 1.30+dfsg-6+deb10u1 CVE ID : CVE-2023-39804 Debian Bug : 1058079

Incorrect handling of extension attributes in PAX archives has been fixed in the GNU tar archiving utility.

For Debian 10 buster, this problem has been fixed in version 1.30+dfsg-6+deb10u1.

We recommend that you upgrade your tar packages.

For the detailed security status of tar please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tar

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/tar
https://security-tracker.debian.org/tracker/CVE-2023-39804
https://packages.debian.org/source/buster/tar

Solution

Upgrade the tar packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-39804

Plugin Information

Published: 2024/03/09, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : tar_1.30+dfsg-6
Should be : tar_1.30+dfsg-6+deb10u1
```

192521 - Debian dla-3771 : idle-python2.7 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3771 advisory.

- ---------- Debian LTS Advisory DLA-3771-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk March 24, 2024 https://wiki.debian.org/LTS
- ----------

Package : python2.7 Version : 2.7.16-2+deb10u4 CVE ID : CVE-2024-0450

The zipfile module was vulnerable to quoted-overlap zip-bombs in the Python 2 interpreter.

For Debian 10 buster, this problem has been fixed in version 2.7.16-2+deb10u4.

We recommend that you upgrade your python2.7 packages.

For the detailed security status of python2.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python2.7

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/python2.7
https://security-tracker.debian.org/tracker/CVE-2024-0450
https://packages.debian.org/source/buster/python2.7

Solution

Upgrade the idle-python2.7 packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2024-0450

Plugin Information

Published: 2024/03/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.16-2+deb10u1
Should be : libpython2.7-minimal_2.7.16-2+deb10u4
Remote package installed : libpython2.7-stdlib_2.7.16-2+deb10u1
Should be : libpython2.7-stdlib_2.7.16-2+deb10u4
Remote package installed : python2.7_2.7.16-2+deb10u1
Should be : python2.7_2.7.16-2+deb10u4
Remote package installed : python2.7-minimal_2.7.16-2+deb10u1
Should be : python2.7-minimal_2.7.16-2+deb10u4
```

197924 - Debian dla-3818 : apache2 - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3818 advisory.

- ---------- Debian LTS Advisory DLA-3818-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris May 24, 2024 https://wiki.debian.org/LTS
- ----------

Package : apache2 Version : 2.4.59-1~deb10u1 CVE ID : CVE-2019-17567 CVE-2023-31122 CVE-2023-38709 CVE-2023-45802 CVE-2024-24795 CVE-2024-27316 Debian Bug : 1068412

Multiple vulnerabilities have been discovered in the Apache HTTP server, which may result in HTTP response splitting, denial of service, or authorization bypass.

CVE-2019-17567

mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

CVE-2023-31122

An Out-of-bounds Read vulnerability was found in mod_macro.

CVE-2023-38709

A faulty input validation was found in the core of Apache that allows malicious or exploitable backend/content generators to split HTTP responses.

CVE-2023-45802

When an HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close.
A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing.
On connection close, all resources were reclaimed, but the process might run out of memory before that.

CVE-2024-24795

HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

CVE-2024-27316

HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

For Debian 10 buster, these problems have been fixed in version 2.4.59-1~deb10u1.

Please note that the fix of CVE-2024-24795, may break unrelated CGI-BIN scripts. As part of the security fix, the Apache webserver mod_cgi module has stopped relaying the Content-Length field of the HTTP reply header from the CGI programs back to the client in cases where the connection is to be closed and the client is able to read until end-of-file. You may restore legacy behavior for trusted scripts by adding the following configuration environment variable to the Apache configuration, scoped to the <Directory> entry or entries in which scripts are being served via CGI, SetEnv ap_trust_cgilike_cl yes.
The definitive fix is to read the whole input, re-allocating the input buffer to fit as more input is received in CGI-BIN scripts, and and to not trust that CONTENT_LENGTH variable is always present.

We recommend that you upgrade your apache2 packages.

For the detailed security status of apache2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/apache2

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/apache2
https://security-tracker.debian.org/tracker/CVE-2019-17567
https://security-tracker.debian.org/tracker/CVE-2023-31122
https://security-tracker.debian.org/tracker/CVE-2023-38709
https://security-tracker.debian.org/tracker/CVE-2023-45802
https://security-tracker.debian.org/tracker/CVE-2024-24795
https://security-tracker.debian.org/tracker/CVE-2024-27316
https://packages.debian.org/source/buster/apache2

Solution

Upgrade the apache2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-17567
CVE	CVE-2023-31122
CVE	CVE-2023-38709
CVE	CVE-2023-45802
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2021-A-0259-S
XREF	IAVA:2023-A-0572-S
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/05/25, Modified: 2024/07/12

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.38-3+deb10u4
Should be : apache2_2.4.59-1~deb10u1
Remote package installed : apache2-bin_2.4.38-3+deb10u4
Should be : apache2-bin_2.4.59-1~deb10u1
Remote package installed : apache2-data_2.4.38-3+deb10u4
Should be : apache2-data_2.4.59-1~deb10u1
Remote package installed : apache2-utils_2.4.38-3+deb10u4
Should be : apache2-utils_2.4.59-1~deb10u1
```

200694 - Debian dla-3831 : nano - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3831 advisory.

- ---------- Debian LTS Advisory DLA-3831-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk June 17, 2024 https://wiki.debian.org/LTS
- ----------

Package : nano Version : 3.2-3+deb10u1 CVE ID : CVE-2024-5742

A symlink attack with emergency file saving has been fixed in the text editor nano.

For Debian 10 buster, this problem has been fixed in version 3.2-3+deb10u1.

We recommend that you upgrade your nano packages.

For the detailed security status of nano please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/nano

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/nano
https://security-tracker.debian.org/tracker/CVE-2024-5742
https://packages.debian.org/source/buster/nano

Solution

Upgrade the nano packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

6.0 (CVSS2#AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2024-5742
XREF	IAVA:2024-A-0355

Plugin Information

Published: 2024/06/18, Modified: 2024/09/25

Plugin Output

tcp/0

```
Remote package installed : nano_3.2-3
Should be : nano_3.2-3+deb10u1
```

201038 - Debian dla-3844 : git - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3844 advisory.

---------- Debian LTS Advisory DLA-3844-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton June 26, 2024 https://wiki.debian.org/LTS

Package : git Version : 1:2.20.1-2+deb10u9 CVE ID : CVE-2019-1387 CVE-2023-25652 CVE-2023-25815 CVE-2023-29007 CVE-2024-32002 CVE-2024-32004 CVE-2024-32021 CVE-2024-32465 Debian Bug : 1034835 1071160

Multiple vulnerabilities were found in git, a fast, scalable and distributed revision control system.

CVE-2019-1387

It was possible to bypass the previous check for this vulnerability using parallel cloning, or the --recurse-submodules option to git-checkout(1).

CVE-2023-25652

Feeding specially-crafted input to 'git apply --reject' could overwrite a path outside the working tree with partially controlled contents, corresponding to the rejected hunk or hunks from the given patch.

CVE-2023-25815

Low-privileged users could inject malicious messages into Git's output under MINGW.

CVE-2023-29007

A specially-crafted .gitmodules file with submodule URLs longer than 1024 characters could be used to inject arbitrary configuration into $GIT_DIR/config.

CVE-2024-32002

Repositories with submodules could be specially-crafted to write hooks into .git/ which would then be executed during an ongoing clone operation.

CVE-2024-32004

A specially-crafted local repository could cause the execution of arbitrary code when cloned by another user.

CVE-2024-32021

When cloning a local repository that contains symlinks via the filesystem, Git could have created hardlinks to arbitrary user-readable files on the same filesystem as the target repository in the objects/ directory.

CVE-2024-32465

When cloning a local repository obtained from a downloaded archive, hooks in that repository could be used for arbitrary code execution.

For Debian 10 buster, these problems have been fixed in version 1:2.20.1-2+deb10u9.

We recommend that you upgrade your git packages.

For the detailed security status of git please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/git

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/git
https://security-tracker.debian.org/tracker/CVE-2019-1387
https://security-tracker.debian.org/tracker/CVE-2023-25652
https://security-tracker.debian.org/tracker/CVE-2023-25815
https://security-tracker.debian.org/tracker/CVE-2023-29007
https://security-tracker.debian.org/tracker/CVE-2024-32002
https://security-tracker.debian.org/tracker/CVE-2024-32004
https://security-tracker.debian.org/tracker/CVE-2024-32021
https://security-tracker.debian.org/tracker/CVE-2024-32465
https://packages.debian.org/source/buster/git

Solution

Upgrade the git packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-1387
CVE	CVE-2023-25652
CVE	CVE-2023-25815
CVE	CVE-2023-29007
CVE	CVE-2024-32002
CVE	CVE-2024-32004
CVE	CVE-2024-32021
CVE	CVE-2024-32465

Plugin Information

Published: 2024/06/26, Modified: 2024/06/26

Plugin Output

tcp/0

```
Remote package installed : git_1:2.20.1-2+deb10u3
Should be : git_1:2.20.1-2+deb10u9
Remote package installed : git-man_1:2.20.1-2+deb10u3
Should be : git-man_1:2.20.1-2+deb10u9
```

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) -

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```

167055 - Debian dla-3181 : sudo - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 10 host has packages installed that are affected by a vulnerability as referenced in the dla-3181 advisory.

- ---------- Debian LTS Advisory DLA-3181-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb November 07, 2022 https://wiki.debian.org/LTS
- ----------

Package : sudo Version : 1.8.27-1+deb10u4 CVE ID : CVE-2021-23239

It was discovered that there was a information disclosure utility in sudo, a tool used to provide limited superuser privileges to specific users.

A local unprivileged user may have been able to perform arbitrary directory-existence tests by exploiting a race condition in sudoedit.

For Debian 10 buster, this problem has been fixed in version 1.8.27-1+deb10u4.

We recommend that you upgrade your sudo packages.

For the detailed security status of sudo please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/sudo

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

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

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

See Also

https://security-tracker.debian.org/tracker/CVE-2021-23239
https://security-tracker.debian.org/tracker/source-package/sudo
https://packages.debian.org/source/buster/sudo

Solution

Upgrade the sudo packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-23239
XREF	IAVA:2021-A-0053

Plugin Information

Published: 2022/11/07, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.27-1+deb10u3
Should be : sudo_1.8.27-1+deb10u4
```

192962 - Debian dla-3782 : bsdutils - security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 10 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3782 advisory.

---------- Debian LTS Advisory DLA-3782-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin April 07, 2024 https://wiki.debian.org/LTS

Package : util-linux Version : 2.33.1-0.1+deb10u1 CVE ID : CVE-2021-37600 CVE-2024-28085 Debian Bug : 826596 991619 1067849

CVE-2024-28085

Skyler Ferrante discovered that the wall(1) utility found in util-linux, a collection of system utilities for Linux, does not filter escape sequences from command line arguments. This allows unprivileged local users to put arbitrary text on other users terminals if mesg is set to y and the wall executable is setgid, which could lead to information disclosure.

With this update the wall executable is no longer installed setgid tty.

CVE-2021-37600

Kihong Heo found an integer overflow which can potentially lead to buffer overflow if an attacker were able to use system resources in a way that leads to a large number in the /proc/sysvipc/sem file.
NOTE: this is issue is unexploitable in GNU C Library environments, and possibly in all realistic environments.

For Debian 10 buster, these problems have been fixed in version 2.33.1-0.1+deb10u1.

We recommend that you upgrade your util-linux packages.

For the detailed security status of util-linux please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/util-linux

Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS Attachment:
signature.asc Description: PGP signature

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

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

See Also

https://security-tracker.debian.org/tracker/source-package/util-linux
https://security-tracker.debian.org/tracker/CVE-2021-37600
https://security-tracker.debian.org/tracker/CVE-2024-28085
https://packages.debian.org/source/buster/util-linux

Solution

Upgrade the bsdutils packages.

Risk Factor

Low

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-37600

CVE CVE-2024-28085

Plugin Information

Published: 2024/04/07, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : fdisk_2.33.1-0.1
Should be : fdisk_2.33.1-0.1+deb10u1
Remote package installed : libblkid1_2.33.1-0.1
Should be : libblkid1_2.33.1-0.1+deb10u1
Remote package installed : libfdisk1_2.33.1-0.1
Should be : libfdisk1_2.33.1-0.1+deb10u1
Remote package installed : libmount1_2.33.1-0.1
Should be : libmount1_2.33.1-0.1+deb10u1
Remote package installed : libsmartcols1_2.33.1-0.1
Should be : libsmartcols1_2.33.1-0.1+deb10u1
Remote package installed : libuuid1_2.33.1-0.1
Should be : libuuid1_2.33.1-0.1+deb10u1
Remote package installed : mount_2.33.1-0.1
Should be : mount_2.33.1-0.1+deb10u1
Remote package installed : util-linux_2.33.1-0.1
Should be : util-linux_2.33.1-0.1+deb10u1
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

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

Description

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0524
XREF CWE:200

Plugin Information

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

Plugin Output

icmp/0

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

141394 - Apache HTTP Server Installed (Linux) -

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/08/19

Plugin Output

tcp/0

```
Path : /usr/sbin/apache2
Version : 2.4.38
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS : True
Running : yes

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 - 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: 2025/07/14

Plugin Output

tcp/0

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

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://10.136.108.235/
Version : 2.4.99
Source : Server: Apache/2.4.38 (Debian)
backported : 1
os : ConvertedDebian
```

156000 - Apache Log4j Installed (Linux / Unix) -

Synopsis

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

Description

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

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

References

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

Plugin Information

Published: 2021/12/10, Modified: 2025/08/18

Plugin Output

tcp/0

```
Path : /usr/share/java/libintl.jar
Version : unknown
JMSAppender.class association : Not Found
JdbcAppender.class association : Not Found
JndiLookup.class association : Not Found
Method : Embedded string inspection

Note: Jar file inspection cannot be performed. No results or cannot list archive contents. If results are present, install an unzip
package to resolve this problem.
```

34098 - BIOS Info (SSH) -

Synopsis

BIOS info could be read.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

39519 - Backported Security Patch Detection (FTP) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

45590 - Common Platform Enumeration (CPE) -

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

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

cpe:/o:debian:debian_linux:10 -> Debian Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.38 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:log4j -> Apache Software Foundation log4j
cpe:/a:docker:docker:18.09.1 -> Docker
cpe:/a:gnupg:libgcrypt:1.8.4 -> GnuPG Libgcrypt
cpe:/a:haxx:libcurl:7.64.0 -> Haxx libcurl
cpe:/a:openbsd:openssh:7.9 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:7.9p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.1.1d -> OpenSSL Project OpenSSL
cpe:/a:tukaani:xz:5.2.4 -> Tukaani XZ
cpe:/a:vim:vim:8.1 -> Vim
```

55472 - Device Hostname -

Synopsis

It was possible to determine the remote system hostname.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/07/28

Plugin Output

tcp/0

```
Hostname : BlueMoon
BlueMoon (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

159488 - 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: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/docker
Version : 18.09.1
```

```
Build : 4c52b90
Managed by OS : True
```

25203 - Enumerate IPv4 Interfaces via SSH -

Synopsis

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

Description

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

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

- 127.0.0.1 (on interface lo)
- 10.136.108.235 (on interface enp0s3)
- 172.17.0.1 (on interface docker0)
```

25202 - Enumerate IPv6 Interfaces via SSH -

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

- ::1 (on interface lo)
- 2409:40c0:52:50ae:a00:27ff:fe43:85f4 (on interface enp0s3)
- fe80::a00:27ff:fe43:85f4 (on interface enp0s3)
- fe80::42:3aff:fe28:debc (on interface docker0)
```

33276 - Enumerate MAC Addresses via SSH -

Synopsis

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

Description

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

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

- 08:00:27:43:85:f4 (interface enp0s3)
- 02:42:3a:28:de:bc (interface docker0)
```

170170 - Enumerate the Network Interface configuration via SSH -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
docker0:
MAC : 02:42:3a:28:de:bc
IPv4:
- Address : 172.17.0.1
Netmask : 255.255.0.0
Broadcast : 172.17.255.255
IPv6:
- Address : fe80::42:3aff:fe28:debc
Prefixlen : 64
Scope : link
lo:
IPv4:
- Address : 127.0.0.1
Netmask : 255.0.0.0
IPv6:
- Address : ::1
Prefixlen : 128
Scope : host
enp0s3:
MAC : 08:00:27:43:85:f4
IPv4:
- Address : 10.136.108.235
Netmask : 255.255.255.0
Broadcast : 10.136.108.255
IPv6:
- Address : 2409:40c0:52:50ae:a00:27ff:fe43:85f4
Prefixlen : 64
Scope : global
- Address : fe80::a00:27ff:fe43:85f4
Prefixlen : 64
Scope : link
```

179200 - Enumerate the Network Routing configuration via SSH -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Gateway Routes:
enp0s3:
ipv4_gateways:
10.136.108.228:
subnets:
- 0.0.0.0/0
ipv6_gateways:
fe80::4a2:97ff:fec8:6a88:
subnets:
- ::/0
Interface Routes:
docker0:
ipv4_subnets:
- 172.17.0.0/16
ipv6_subnets:
- fe80::/64
enp0s3:
ipv4_subnets:
- 10.136.108.0/24
ipv6_subnets:
- 2409:40c0:52:50ae::/64
- fe80::/64
```

168980 - Enumerate the PATH Variables -

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

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

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/07/28

Plugin Output

tcp/0

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

/usr/local/bin
/usr/bin
/bin
/usr/games
```

35716 - Ethernet Card Manufacturer Detection -

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:43:85:F4 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- 08:00:27:43:85:F4
- 02:42:3A:28:DE:BC
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 3.0.3)
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.38 (Debian)
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

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

Date: Sat, 15 Nov 2025 16:43:02 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Sun, 04 Apr 2021 14:25:48 GMT
ETag: "17f-5bf265b88ecc3"
Accept-Ranges: bytes
Content-Length: 383
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!doctype html>
<html>
<head>
<title>BlueMoon:2021</title>
```

```
<link rel="icon" href=".blue.jpg" type="image/icon type">
</head>

<body>
<div>
<h1>" -- Welcome -- "</h1><br>
<p><b>Are You Ready To Play With Me .....!</b></p>
<br>
<p style="text-align:center;"><img src=".starts.jpeg" alt="Target" style="width:600px;height:400px;"></p>
</div>
</body>
</html>
```

171410 - IP Assignment Method Detection -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ enp0s3
+ IPv4
- Address : 10.136.108.235
Assign Method : dynamic
+ IPv6
- Address : 2409:40c0:52:50ae:a00:27ff:fe43:85f4
Assign Method : dynamic
- Address : fe80::a00:27ff:fe43:85f4
Assign Method : static
+ docker0
+ IPv4
- Address : 172.17.0.1
Assign Method : static
+ IPv6
- Address : fe80::42:3aff:fe28:debc
Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX) -

Synopsis

Libgcrypt is installed on this host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

Path : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.8.4

Path : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.4
Version : 1.8.4

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.8.4

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20.2.4
Version : 1.8.4
```

157358 - Linux Mounted Devices -

Synopsis

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

Description

Report the mounted devices information on the target machine at scan time using the following commands.
/bin/df -h /bin/lsblk /bin/mount -l

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 479M 0 479M 0% /dev
tmpfs 99M 4.2M 95M 5% /run
/dev/mapper/Target--vg-root 6.4G 1.4G 4.7G 23% /
tmpfs 494M 0 494M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 494M 0 494M 0% /sys/fs/cgroup
/dev/sda1 472M 49M 399M 11% /boot
tmpfs 99M 0 99M 0% /run/user/1002


$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 8G 0 disk
├─sda1 8:1 0 487M 0 part /boot
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 7.5G 0 part
├─Target--vg-root 254:0 0 6.6G 0 lvm /
└─Target--vg-swap_1 254:1 0 980M 0 lvm [SWAP]
sr0 11:0 1 1024M 0 rom


$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=489556k,nr_inodes=122389,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=101108k,mode=755)
/dev/mapper/Target--vg-root on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
```

```
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
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)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
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=10632)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
/dev/sda1 on /boot type ext2 (rw,relatime)
tmpfs on /run/user/1002 type tmpfs (rw,nosuid,nodev,relatime,size=101104k,mode=700,uid=1002,gid=1002)
```

193143 - Linux Time Zone Information -

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Via date: PST -0800
Via timedatectl: Time zone: US/Pacific (PST, -0800)
Via /etc/timezone: US/Pacific
Via /etc/localtime: PST8PDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration -

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

User : robin
```

```
Home folder : /home/robin
Start script : /bin/bash
Groups : video
cdrom
netdev
floppy
robin
plugdev
dip
audio

User : userftp
Home folder : /home/userftp
Start script : /bin/sh
Groups : userftp

User : jerry
Home folder : /home/jerry
Start script : /bin/bash
Groups : jerry
docker

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
User : irc
Home folder : /var/run/ircd
Start script : /usr/sbin/nologin
Groups : irc

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

User : nobody
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : _apt
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : systemd-timesync
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-timesync

User : systemd-network
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-network

User : systemd-resolve
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-resolve

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

User : messagebus
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : messagebus

User : sshd
Home folder : /run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup

User : ftp
Home folder : /srv/ftp
Start script : /usr/sbin/nologin
Groups : ftp


----------[ Domain Accounts ]----------
```

19506 - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : BlueMoon
Scan policy used : Advanced Scan
Scanner IP : 10.136.108.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 310.155 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'jerry' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/11/15 16:42 UTC
Scan duration : 404 sec
Scan for malware : no
```

64582 - Netstat Connection Information -

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

209654 - OS Fingerprints Detected -

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

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

Remote operating system : Linux Kernel 4.19.0-14-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux BlueMoon 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux


Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W64240:O0204ffff:M1460:
P2:B10113:F0x12:W65160:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191303_7_p=22

Remote operating system : Linux Kernel 4.19.0-14-amd64 on Debian 10.8
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
SSH:!:SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
HTTP:!:Server: Apache/2.4.38 (Debian)
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.19.0-14-amd64 on Debian 10.8
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 4.19.0-14-amd64 on Debian 10.8
```

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

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

The output of "uname -a" is :
Linux BlueMoon 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
10.8

OS Security Patch Assessment is available for this host.
Runtime : 5.10258 seconds
```

117887 - OS Security Patch Assessment Available -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

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

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account : jerry
Protocol : SSH
```

181418 - OpenSSH Detection -

Synopsis

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

Description

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

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.9p1
Banner : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

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

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

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

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 3 installs of OpenSSL:

Path : /usr/lib/x86_64-linux-gnu/libssl.so.1.1
Version : 1.1.1d
Associated Package : libssl1.1

Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
Version : 1.1.1d
Associated Package : libssl1.1

Path : /usr/bin/openssl
```

```
Version : 1.1.1d
Associated Package : openssl 1.1.1d-0
Managed by OS : True
```

179139 - Package Manager Packages Report (nix) -

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

```
. You need to take the following 53 actions :

[ Debian DSA-4875-1 : openssl - security update (148170) ]

+ Action to take : Upgrade the openssl packages.

For the stable distribution (buster), this problem has been fixed in version 1.1.1d-0+deb10u6.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Debian DSA-4919-1 : lz4 - security update (149855) ]

+ Action to take : Upgrade the lz4 packages.

For the stable distribution (buster), this problem has been fixed in version 1.8.3-1+deb10u1.
```

[Debian DSA-4920-1 : libx11 - security update (149897)]

+ Action to take : Upgrade the libx11 packages.

For the stable distribution (buster), this problem has been fixed in version 2:1.6.7-1+deb10u2.

[Debian DSA-4933-1 : nettle - security update (150905)]

+ Action to take : Upgrade the nettle packages.

For the stable distribution (buster), these problems have been fixed in version 3.4.1-1+deb10u1.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DSA-5014-1 : icu - security update (155709)]

+ Action to take : Upgrade the icu packages.

[Debian DSA-5087-1 : cyrus-sasl2 - security update (158509)]

+ Action to take : Upgrade the cyrus-sasl2 packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.1.27+dfsg-2.1+deb11u1.

[Debian DSA-5096-1 : linux - security update (158761)]

+ Action to take : Upgrade the linux packages.

+Impact : Taking this action will resolve 52 different vulnerabilities (CVEs).

[Debian DSA-5122-1 : gzip - security update (159906)]

+ Action to take : Upgrade the gzip packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.10-4+deb11u1.

[Debian DSA-5123-1 : xz-utils - security update (159904)]

+ Action to take : Upgrade the xz-utils packages.

For the stable distribution (bullseye), this problem has been fixed in version 5.2.5-2.1~deb11u1.

[Debian DSA-5137-1 : needrestart - security update (161254)]

+ Action to take : Upgrade the needrestart packages.

For the stable distribution (bullseye), this problem has been fixed in version 3.5-4+deb11u1.

[Debian DSA-5140-1 : openldap - security update (161404)]

+ Action to take : Upgrade the openldap packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.4.57+dfsg-3+deb11u1.

[Debian DSA-5147-1 : dpkg - security update (161513)]

+ Action to take : Upgrade the dpkg packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.20.10.

[Debian DSA-5150-1 : rsyslog - security update (161689)]

+ Action to take : Upgrade the rsyslog packages.

For the stable distribution (bullseye), this problem has been fixed in version 8.2102.0-2+deb11u1.

[Debian DSA-5169-1 : openssl - security update (162549)]

+ Action to take : Upgrade the openssl packages.

For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u3.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Debian DSA-5174-1 : gnupg2 - security update (162701)]

+ Action to take : Upgrade the gnupg2 packages.

For the stable distribution (bullseye), this problem has been fixed in version 2.2.27-2+deb11u2.

[Debian dla-3103 : lib32z1 - security update (164946)]

+ Action to take : Upgrade the lib32z1 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian dla-3107 : lemon - security update (164992)]

+ Action to take : Upgrade the lemon packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian dla-3146 : isc-dhcp-client - security update (166004)]

+ Action to take : Upgrade the isc-dhcp-client packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian dla-3263 : libtasn1-6 - security update (169736)]

+ Action to take : Upgrade the libtasn1-6 packages.

[Debian dla-3332 : libaprutil1 - security update (171753)]

+ Action to take : Upgrade the libaprutil1 packages.

[Debian dla-3363 : libpcre2-16-0 - security update (172599)]

+ Action to take : Upgrade the libpcre2-16-0 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian dla-3405 : libxml2 - security update (174964)]

+ Action to take : Upgrade the libxml2 packages.

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

[Debian dla-3445 : cpio - security update (176664)]

+ Action to take : Upgrade the cpio packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian dla-3461 : libfastjson-dev - security update (177513)]

+ Action to take : Upgrade the libfastjson-dev packages.

[Debian dla-3474 : libnss-myhostname - security update (177792)]

+ Action to take : Upgrade the libnss-myhostname packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian dla-3530 : libssl-dev - security update (179900)]

+ Action to take : Upgrade the libssl-dev packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Debian dla-3559 : libssh2-1 - security update (181187)]

+ Action to take : Upgrade the libssh2-1 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian dla-3579 : elfutils - security update (181835)]

+ Action to take : Upgrade the elfutils packages.

[Debian dla-3588 : vim - security update (182369)]

+ Action to take : Upgrade the vim packages.

+Impact : Taking this action will resolve 58 different vulnerabilities (CVEs).

[Debian dla-3602 : libx11-6 - security update (182584)]

+ Action to take : Upgrade the libx11-6 packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian dla-3605 : grub-common - security update (182650)]

+ Action to take : Upgrade the grub-common packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian dla-3626 : krb5-admin-server - security update (183680)]

+ Action to take : Upgrade the krb5-admin-server packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian dla-3628 : dbus - security update (183747)]

+ Action to take : Upgrade the dbus packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian dla-3682 : lib32ncurses-dev - security update (186526)]

+ Action to take : Upgrade the lib32ncurses-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian dla-3694 : openssh-client - security update (214473)]

+ Action to take : Upgrade the openssh-client packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian dla-3732 : sudo - security update (189972)]

+ Action to take : Upgrade the sudo packages.

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

[Debian dla-3735 : golang-github-opencontainers-runc-dev - security update (190686)]

+ Action to take : Upgrade the golang-github-opencontainers-runc-dev packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Debian dla-3740 : gnutls-bin - security update (190998)]

+ Action to take : Upgrade the gnutls-bin packages.

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

[Debian dla-3755 : tar - security update (191776)]

+ Action to take : Upgrade the tar packages.

[Debian dla-3757 : libnss3 - security update (191787)]

+ Action to take : Upgrade the libnss3 packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Debian dla-3763 : curl - security update (192185)]

+ Action to take : Upgrade the curl packages.

+Impact : Taking this action will resolve 32 different vulnerabilities (CVEs).

[Debian dla-3771 : idle-python2.7 - security update (192521)]

+ Action to take : Upgrade the idle-python2.7 packages.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

```
[ Debian dla-3772 : idle-python3.7 - security update (192520) ]

+ Action to take : Upgrade the idle-python3.7 packages.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).


[ Debian dla-3782 : bsdutils - security update (192962) ]

+ Action to take : Upgrade the bsdutils packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian dla-3783 : expat - security update (193076) ]

+ Action to take : Upgrade the expat packages.

+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).


[ Debian dla-3804 : libnghttp2-14 - security update (194852) ]

+ Action to take : Upgrade the libnghttp2-14 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Debian dla-3816 : bind9 - security update (197488) ]

+ Action to take : Upgrade the bind9 packages.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).


[ Debian dla-3818 : apache2 - security update (197924) ]

+ Action to take : Upgrade the apache2 packages.

+Impact : Taking this action will resolve 23 different vulnerabilities (CVEs).


[ Debian dla-3823 : less - security update (197941) ]

+ Action to take : Upgrade the less packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian dla-3831 : nano - security update (200694) ]

+ Action to take : Upgrade the nano packages.

[ Debian dla-3844 : git - security update (201038) ]

+ Action to take : Upgrade the git packages.

+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).


[ Debian dla-3850 : glibc-doc - security update (201168) ]

+ Action to take : Upgrade the glibc-doc packages.

+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).


[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.
```

45405 - Reachable IPv6 address -

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2024/07/24

Plugin Output

tcp/0

```
The following global address was gathered :

- 2409:40c0:52:50ae:a00:27ff:fe43:85f4
```

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

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

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
```

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

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for kex_algorithms :

curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation -

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0507

Plugin Information

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

Plugin Output

tcp/0

```
Login account : jerry
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
```

```
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\n/dev/mem: Permission denied"
- Command : "LC_ALL=C /sbin/dmidecode"
Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\n/dev/mem: Permission denied"
- Plugin Filename : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
- Command : "/usr/sbin/dmidecode -s system-version 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : enumerate_oci_nix.nasl
Plugin ID : 154138
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Command : "LC_ALL=C /sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : host_tag_nix.nbin
Plugin ID : 87414
Plugin Name : Host Tagging (Linux)
- Command : "sh -c \"echo 3a118f7065bc4e4daae98ef8a9808b0b > /etc/tenable_tag && echo OK\""
Response : null
Error : "\nsh: 1: \ncannot create /etc/tenable_tag: Permission denied"
- Plugin Filename : linux_kernel_speculative_execution_detect.nbin
Plugin ID : 125216
Plugin Name : Processor Speculative Execution Vulnerabilities (Linux)
- Command : "head /sys/kernel/debug/x86/pti_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/pti_enabled' for reading\n: Permission denied"
- Command : "head /sys/kernel/debug/x86/retp_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/retp_enabled' for reading\n: Permission denied"
- Command : "head /sys/kernel/debug/x86/ibrs_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/ibrs_enabled' for reading\n: Permission denied"
- Plugin Filename : localusers_pwexpiry.nasl
Plugin ID : 83303
Plugin Name : Unix / Linux - Local Users Information : Passwords Never Expire
- Command : "cat /etc/shadow"
Response : null
Error : "\ncat: \n/etc/shadow\n: Permission denied"
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

- 1.99
- 2.0
```

90707 - SSH SCP Protocol Detection -

Synopsis

The remote host supports the SCP protocol over SSH.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

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

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

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH supported authentication : publickey,password
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22869 - Software Enumeration (SSH) -

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

ii adduser 3.118 all add and remove users and groups
ii apache2 2.4.38-3+deb10u4 amd64 Apache HTTP Server
ii apache2-bin 2.4.38-3+deb10u4 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.38-3+deb10u4 all Apache HTTP Server (common files)
ii apache2-utils 2.4.38-3+deb10u4 amd64 Apache HTTP Server (utility programs for web servers)
ii apparmor 2.13.2-10 amd64 user-space parser utility for AppArmor
ii apt 1.8.2.2 amd64 commandline package manager
ii apt-utils 1.8.2.2 amd64 package management related utility programs
ii base-files 10.3+deb10u8 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.46 amd64 Debian base system master password and group files
ii bash 5.0-4 amd64 GNU Bourne Again SHell
ii binutils 2.31.1-16 amd64 GNU assembler, linker and binary utilities
ii binutils-common 2.31.1-16 amd64 Common files for the GNU assembler, linker and binary utilities
ii binutils-x86-64-linux-gnu 2.31.1-16 amd64 GNU binary utilities, for x86-64-linux-gnu target
ii bsdmainutils 11.1.2+b1 amd64 collection of more utilities from FreeBSD
ii bsdutils 1:2.33.1-0.1 amd64 basic utilities from 4.4BSD-Lite
ii busybox 1:1.30.1-4 amd64 Tiny utilities for small and embedded systems
ii bzip2 1.0.6-9.2~deb10u1 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20200601~deb10u2 all Common CA certificates
ii cgroupfs-mount 1.4 all Light-weight package to set up cgroupfs mounts
ii console-setup 1.193~deb10u1 all console font and keymap setup program
ii console-setup-linux 1.193~deb10u1 all Linux specific part of console-setup
ii coreutils 8.30-3 amd64 GNU core utilities
ii cpio 2.12+dfsg-9 amd64 GNU cpio -- a program to manage archives of files
ii cron 3.0pl1-134+deb10u1 amd64 process scheduling daemon
ii dash 0.5.10.2-5 amd64 POSIX-compliant shell
ii dbus 1.12.20-0+deb10u1 amd64 simple interprocess messaging system (daemon and utilities)
ii debconf 1.5.71 all Debian configuration management system
ii debconf-i18n 1.5.71 all full internationalization support for debconf
ii debian-archive-keyring 2019.1 all GnuPG archive keys of the Debian archive
ii debianutils 4.8.6.1 amd64 Miscellaneous utilities specific to Debian
ii diffutils 1:3.7-3 amd64 File comparison utilities
ii dmeventd 2:1.02.155-3 amd64 Linux Kernel Device Mapper event daemon
ii dmidecode 3.2-1 amd64 SMBIOS/DMI table decoder
ii dmsetup 2:1.02.155-3 amd64 Linux Kernel Device Mapper userspace library
ii docker.io 18.09.1+dfsg1-7.1+deb10u3 amd64 Linux container runtime
ii dpkg 1.19.7 amd64 Debian package management system
ii e2fsprogs 1.44.5-1+deb10u3 amd64 ext2/ext3/ext4 file system utilities
ii eject 2.1.5+deb1+cvs20081104-13.2 amd64 ejects CDs and operates CD-Changers under Linux
ii fdisk 2.33.1-0.1 amd64 collection of partitioning utilities
ii file 1:5.35-4+deb10u2 amd64 Recognize the type of data in a file using "magic" numbers
ii findutils 4.6.0+git+20190209-2 amd64 utilities for finding files--find, xargs
ii firmware-linux-free 3.4 all Binary firmware for various drivers in the Linux kernel
ii gcc-8-base 8.3.0-6 amd64 GCC, the GNU Compiler Collection (base package)
ii gdbm-l10n 1.18.1-4 all GNU dbm database routines (translation files)
ii gettext-base 0.19.8.1-9 amd64 GNU Internationalization utilities for the base system
ii git 1:2.20.1-2+deb10u3 amd64 fast, scalable, distributed revision control system
ii git-man 1:2.20.1-2+deb10u3 all fast, scalable, distributed revision control system (manual pages)
ii gpgv 2.2.12-1+deb10u1 amd64 GNU privacy guard - signature verification tool
ii grep 3.3-1 amd64 GNU grep, egrep and fgrep
ii grub-common 2.02+dfsg1-20+deb10u4 amd64 GRand Unified Bootloader (common files)
ii grub-pc 2.02+dfsg1-20+deb10u4 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 2.02+dfsg1-20+deb10u4 amd64 GRand Unified Bootloader, version 2 (PC/BIOS modules)
ii grub2-common 2.02+dfsg1-20+deb10u4 amd64 GRand Unified Bootloader (common files for version 2)
ii gzip 1.9-3 amd64 GNU compression utilities
ii hostname 3.21 amd64 utility to set/show the host name or domain name
ii ifupdown 0.8.35 amd64 high level tools to configure network interfaces
ii init 1.56+nmu1 amd64 metapackage ensuring an init system is installed
ii init-system-helpers 1.56+nmu1 all helper tools for all init systems
ii initramfs-tools 0.133+deb10u1 all generic modular initramfs generator (automation)
ii initramfs-tools-core 0.133+deb10u1 all generic modular initramfs generator (core tools)
ii iproute2 4.20.0-2+deb10u1 amd64 networking and traffic control tools
ii iptables 1.8.2-4 amd64 administration tools for packet filtering and NAT
ii iputils-ping 3:20180629-2+deb10u1 amd64 Tools to test the reachability of network hosts
ii isc-dhcp-client 4.4.1-2 amd64 DHCP client for automatically obtaining an IP address
ii isc-dhcp-common 4.4.1-2 amd64 common manpages relevant to all of the isc-dhcp packages
ii kbd 2.0.4-4 amd64 Linux console font and keytable utilities
ii keyboard-configuration 1.193~deb10u1 all system-wide keyboard preferences
ii klibc-utils 2.0.6-1 amd64 small utilities built with klibc for early boot
ii kmod 26-1 amd64 tools for managing Linux kernel modules
ii krb5-locales 1.17-3+deb10u1 all internationalization support for MIT Kerberos
ii less 487-0.1+b1 amd64 pager program similar to more
ii libacl1 2.2.53-4 amd64 access control list - shared library
ii libaio1 0.3.112-3 amd64 Linux kernel AIO access library - shared library
ii libapparmor1 2.13.2-10 amd64 changehat AppArmor library
ii libapr1 1.6.5-1+b1 amd64 Apache Portable Runtime Library
ii libaprutil1 1.6.1-4 amd64 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.6.1-4 amd64 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.6.1-4 amd64 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-inst2.0 1.8.2.2 amd64 deb package format runtime library
ii libapt-pkg5.0 1.8.2.2 amd64 package management runtime library
ii libargon2-1 0~20171227-0.2 amd64 memory-hard hashing function - runtime library
ii libattr1 1:2.4.48-4 amd64 extended attribute handling - shared library
ii libaudit-common 1:2.8.4-3 all Dynamic library for security auditing - common files
ii libaudit1 1:2.8.4-3 amd64 Dynamic library for security auditing
ii libbinutils 2.31.1-16 amd64 GNU binary utilities (private shared library)
ii libblkid1 2.33.1-0.1 amd64 block device ID library
ii libbrotli1 1.0.7-2+deb10u1 amd64 library implementing brotli encoder and decoder (shared libraries)
```

```
ii libbsd0 0.9.1-2 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-9.2~deb10u1 amd64 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.28-10 amd64 GNU C Library: Binaries
ii libc-l10n 2.28-10 all GNU C Library: localization files
ii libc6 2.28-10 amd64 GNU C Library: Shared libraries
ii libcap-ng0 0.7.9-2 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.25-2 amd64 POSIX 1003.1e capabilities (library)
ii libcap2-bin 1:2.25-2 amd64 POSIX 1003.1e capabilities (utilities)
ii libcom-err2 1.44.5-1+deb10u3 amd64 common error description library
ii libcryptsetup12 2:2.1.0-5+deb10u2 amd64 disk encryption support - shared library
ii libcurl3-gnutls 7.64.0-4+deb10u1 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libcurl4 7.64.0-4+deb10u1 amd64 easy-to-use client-side URL transfer library (OpenSSL flavour)
ii libdb5.3 5.3.28+dfsg1-0.5 amd64 Berkeley v5.3 Database Libraries [runtime]
ii libdbus-1-3 1.12.20-0+deb10u1 amd64 simple interprocess messaging system (library)
ii libdebconfclient0 0.249 amd64 Debian Configuration Management System (C-implementation library)
ii libdevmapper-event1.02.1 2:1.02.155-3 amd64 Linux Kernel Device Mapper event support library
ii libdevmapper1.02.1 2:1.02.155-3 amd64 Linux Kernel Device Mapper userspace library
ii libdns-export1104 1:9.11.5.P4+dfsg-5.1+deb10u2 amd64 Exported DNS Shared Library
ii libedit2 3.1-20181209-1 amd64 BSD editline and history libraries
ii libefiboot1 37-2+deb10u1 amd64 Library to manage UEFI variables
ii libefivar1 37-2+deb10u1 amd64 Library to manage UEFI variables
ii libelf1 0.176-1.1 amd64 library to read and write ELF files
ii liberror-perl 0.17027-2 all Perl module for error/exception handling in an OO-ish way
ii libestr0 0.1.10-2.1 amd64 Helper functions for handling strings (lib)
ii libexpat1 2.2.6-2+deb10u1 amd64 XML parsing C library - runtime library
ii libext2fs2 1.44.5-1+deb10u3 amd64 ext2/ext3/ext4 file system libraries
ii libfastjson4 0.99.8-2 amd64 fast json library for C
ii libfdisk1 2.33.1-0.1 amd64 fdisk partitioning library
ii libffi6 3.2.1-9 amd64 Foreign Function Interface library runtime
ii libfreetype6 2.9.1-3+deb10u2 amd64 FreeType 2 font engine, shared library files
ii libfuse2 2.9.9-1+deb10u1 amd64 Filesystem in Userspace (library)
ii libgcc1 1:8.3.0-6 amd64 GCC support library
ii libgcrypt20 1.8.4-5 amd64 LGPL Crypto library - runtime library
ii libgdbm-compat4 1.18.1-4 amd64 GNU dbm database routines (legacy support runtime version)
ii libgdbm6 1.18.1-4 amd64 GNU dbm database routines (runtime version)
ii libgmp10 2:6.1.2+dfsg-4 amd64 Multiprecision arithmetic library
ii libgnutls30 3.6.7-4+deb10u6 amd64 GNU TLS library - main runtime library
ii libgpg-error0 1.35-1 amd64 GnuPG development runtime library
ii libgssapi-krb5-2 1.17-3+deb10u1 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libhogweed4 3.4.1-1 amd64 low level cryptographic library (public-key cryptos)
ii libicu63 63.1-6+deb10u1 amd64 International Components for Unicode
ii libidn11 1.33-2.2 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libidn2-0 2.0.5-1+deb10u1 amd64 Internationalized domain names (IDNA2008/TR46) library
ii libintl-perl 1.26-2 all Uniforum message translations system compatible i18n library
ii libintl-xs-perl 1.26-2+b4 amd64 Uniforum message translations system compatible i18n library
ii libip4tc0 1.8.2-4 amd64 netfilter libip4tc library
ii libip6tc0 1.8.2-4 amd64 netfilter libip6tc library
ii libiptc0 1.8.2-4 amd64 netfilter libiptc library
ii libisc-export1100 1:9.11.5.P4+dfsg-5.1+deb10u2 amd64 Exported ISC Shared Library
ii libjansson4 2.12-1 amd64 C library for encoding, decoding and manipulating JSON data
ii libjson-c3 0.12.1+ds-2+deb10u1 amd64 JSON manipulation library - shared library
ii libk5crypto3 1.17-3+deb10u1 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.6-6 amd64 Linux Key Management Utilities (library)
ii libklibc 2.0.6-1 amd64 minimal libc subset for use with initramfs
ii libkmod2 26-1 amd64 libkmod shared library
ii libkrb5-3 1.17-3+deb10u1 amd64 MIT Kerberos runtime libraries
ii libkrb5support0 1.17-3+deb10u1 amd64 MIT Kerberos runtime libraries - Support library
ii libldap-2.4-2 2.4.47+dfsg-3+deb10u6 amd64 OpenLDAP libraries
ii libldap-common 2.4.47+dfsg-3+deb10u6 all OpenLDAP common files for libraries
ii liblocale-gettext-perl 1.07-3+b4 amd64 module using libc functions for internationalization in Perl
ii liblognorm5 2.0.5-1 amd64 log normalizing library
ii libltdl7 2.4.6-9 amd64 System independent dlopen wrapper for GNU libtool
ii liblua5.2-0 5.2.4-1.1+b2 amd64 Shared library for the Lua interpreter version 5.2
ii liblvm2cmd2.03 2.03.02-3 amd64 LVM2 command library
ii liblz4-1 1.8.3-1 amd64 Fast LZ compression algorithm library - runtime
ii liblzma5 5.2.4-1 amd64 XZ-format compression library
ii libmagic-mgc 1:5.35-4+deb10u2 amd64 File type determination library using "magic" numbers (compiled magic file)
ii libmagic1 1:5.35-4+deb10u2 amd64 Recognize the type of data in a file using "magic" numbers - library
ii libmnl0 1.0.4-2 amd64 minimalistic Netlink communication library
ii libmodule-find-perl 0.13-1 all module to find and use installed Perl modules
ii libmodule-scandeps-perl 1.27-1 all module to recursively scan Perl code for dependencies
ii libmount1 2.33.1-0.1 amd64 device mounting library
ii libmpdec2 2.4.2-2 amd64 library for decimal floating point arithmetic (runtime library)
ii libncurses6 6.1+20181013-2+deb10u2 amd64 shared libraries for terminal handling
ii libncursesw6 6.1+20181013-2+deb10u2 amd64 shared libraries for terminal handling (wide character support)
ii libnetfilter-conntrack3 1.0.7-1 amd64 Netfilter netlink-conntrack library
ii libnettle6 3.4.1-1 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52.20-8 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.1-3+b1 amd64 Netfilter netlink library
ii libnftnl11 1.1.2-2 amd64 Netfilter nftables userspace API library
ii libnghttp2-14 1.36.0-2+deb10u1 amd64 library implementing HTTP/2 protocol (shared library)
ii libnspr4 2:4.20-1 amd64 NetScape Portable Runtime Library
ii libnss3 2:3.42.1-1+deb10u3 amd64 Network Security Service libraries
ii libp11-kit0 0.23.15-2+deb10u1 amd64 library for loading and coordinating access to PKCS#11 modules - runtime
ii libpam-modules 1.3.1-5 amd64 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.3.1-5 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.3.1-5 all Runtime support for the PAM library
ii libpam-systemd 241-7~deb10u6 amd64 system and service manager - PAM module
ii libpam0g 1.3.1-5 amd64 Pluggable Authentication Modules library
ii libpci3 1:3.5.2-1 amd64 Linux PCI Utilities (shared library)
ii libpcre2-8-0 10.32-5 amd64 New Perl Compatible Regular Expression Library- 8 bit runtime files
ii libpcre3 2:8.39-12 amd64 Old Perl 5 Compatible Regular Expression Library - runtime files
ii libperl5.28 5.28.1-6+deb10u1 amd64 shared Perl library
ii libpng16-16 1.6.36-6 amd64 PNG library - runtime (version 1.6)
ii libpopt0 1.16-12 amd64 lib for parsing cmdline parameters
ii libproc-processtable-perl 0.56-1 amd64 Perl library for accessing process table information
ii libprocps7 2:3.3.15-2 amd64 library for accessing process information from /proc
ii libpsl5 0.20.2-2 amd64 Library for Public Suffix List (shared libraries)
ii libpython-stdlib 2.7.16-1 amd64 interactive high-level object-oriented language (Python2)
```

```
ii libpython2-stdlib 2.7.16-1 amd64 interactive high-level object-oriented language (Python2)
ii libpython2.7-minimal 2.7.16-2+deb10u1 amd64 Minimal subset of the Python language (version 2.7)
ii libpython2.7-stdlib 2.7.16-2+deb10u1 amd64 Interactive high-level object-oriented language (standard library, version 2.7)
ii libpython3-stdlib 3.7.3-1 amd64 interactive high-level object-oriented language (default python3 version)
ii libpython3.7-minimal 3.7.3-2+deb10u2 amd64 Minimal subset of the Python language (version 3.7)
ii libpython3.7-stdlib 3.7.3-2+deb10u2 amd64 Interactive high-level object-oriented language (standard library, version 3.7)
ii libreadline5 5.2+dfsg-3+b13 amd64 GNU readline and history libraries, run-time libraries
ii libreadline7 7.0-5 amd64 GNU readline and history libraries, run-time libraries
ii librtmp1 2.4+20151223.gitfa8646d.1-2 amd64 toolkit for RTMP streams (shared library)
ii libsasl2-2 2.1.27+dfsg-1+deb10u1 amd64 Cyrus SASL - authentication abstraction library
ii libsasl2-modules 2.1.27+dfsg-1+deb10u1 amd64 Cyrus SASL - pluggable authentication modules
ii libsasl2-modules-db 2.1.27+dfsg-1+deb10u1 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii libseccomp2 2.3.3-4 amd64 high level interface to Linux seccomp filter
ii libselinux1 2.8-1+b1 amd64 SELinux runtime shared libraries
ii libsemanage-common 2.8-2 all Common files for SELinux policy management libraries
ii libsemanage1 2.8-2 amd64 SELinux policy management library
ii libsepol1 2.8-1 amd64 SELinux library for manipulating binary security policies
ii libslang2 2.3.2-2 amd64 S-Lang programming library - runtime version
ii libsmartcols1 2.33.1-0.1 amd64 smart column output alignment library
ii libsort-naturally-perl 1.03-2 all Sort naturally - sort lexically except for numerical parts
ii libsqlite3-0 3.27.2-3+deb10u1 amd64 SQLite 3 shared library
ii libss2 1.44.5-1+deb10u3 amd64 command-line interface parsing library
ii libssh2-1 1.8.0-2.1 amd64 SSH2 client-side library
ii libssl1.1 1.1.1d-0+deb10u4 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstdc++6 8.3.0-6 amd64 GNU Standard C++ Library v3
ii libsystemd0 241-7~deb10u6 amd64 systemd utility library
ii libtasn1-6 4.13-3 amd64 Manage ASN.1 structures (runtime)
ii libterm-readkey-perl 2.38-1 amd64 perl module for simple terminal control
ii libtext-charwidth-perl 0.04-7.1+b1 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5+b7 amd64 converts between character sets in Perl
ii libtext-wrapi18n-perl 0.06-7.1 all internationalized substitute of Text::Wrap
ii libtinfo6 6.1+20181013-2+deb10u2 amd64 shared low-level terminfo library for terminal handling
ii libudev1 241-7~deb10u6 amd64 libudev shared library
ii libunistring2 0.9.10-1 amd64 Unicode string library for C
ii libusb-1.0-0 2:1.0.22-2 amd64 userspace USB programming library
ii libuuid1 2.33.1-0.1 amd64 Universally Unique ID library
ii libwrap0 7.6.q-28 amd64 Wietse Venema's TCP wrappers library
ii libx11-6 2:1.6.7-1+deb10u1 amd64 X11 client-side library
ii libx11-data 2:1.6.7-1+deb10u1 all X11 client-side library
ii libxau6 1:1.0.8-1+b2 amd64 X11 authorisation library
ii libxcb1 1.13.1-2 amd64 X C Binding
ii libxdmcp6 1:1.1.2-3 amd64 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.3-1+b2 amd64 X11 miscellaneous extension library
ii libxml2 2.9.4+dfsg1-7+deb10u1 amd64 GNOME XML library
ii libxmuu1 2:1.1.2-2+b3 amd64 X11 miscellaneous micro-utility library
ii libxtables12 1.8.2-4 amd64 netfilter xtables library
ii libzstd1 1.3.8+dfsg-3 amd64 fast lossless compression algorithm
ii linux-base 4.6 all Linux image base package
ii linux-image-4.19.0-14-amd64 4.19.171-2 amd64 Linux 4.19 for 64-bit PCs (signed)
ii linux-image-amd64 4.19+105+deb10u9 amd64 Linux for 64-bit PCs (meta-package)
ii locales 2.28-10 all GNU C Library: National Language (locale) data [support]
ii login 1:4.5-1.1 amd64 system login tools
ii logrotate 3.14.0-4 amd64 Log rotation utility
ii lsb-base 10.2019051400 all Linux Standard Base init script functionality
ii lvm2 2.03.02-3 amd64 Linux Logical Volume Manager
ii mawk 1.3.3-17+b3 amd64 a pattern scanning and text processing language
ii mime-support 3.62 all MIME files 'mime.types' & 'mailcap', and support programs
ii mount 2.33.1-0.1 amd64 tools for mounting and manipulating filesystems
ii nano 3.2-3 amd64 small, friendly text editor inspired by Pico
ii ncurses-base 6.1+20181013-2+deb10u2 all basic terminal type definitions
ii ncurses-bin 6.1+20181013-2+deb10u2 amd64 terminal-related programs and man pages
ii ncurses-term 6.1+20181013-2+deb10u2 all additional terminal type definitions
ii needrestart 3.4-5 all check which daemons need to be restarted after library upgrades
ii netbase 5.6 all Basic TCP/IP networking system
ii openssh-client 1:7.9p1-10+deb10u2 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:7.9p1-10+deb10u2 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:7.9p1-10+deb10u2 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines
ii openssl 1.1.1d-0+deb10u5 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii os-prober 1.77 amd64 utility to detect other OSes on a set of drives
ii passwd 1:4.5-1.1 amd64 change and administer password and group data
ii patch 2.7.6-3+deb10u1 amd64 Apply a diff file to an original
ii pciutils 1:3.5.2-1 amd64 Linux PCI Utilities
ii perl 5.28.1-6+deb10u1 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.28.1-6+deb10u1 amd64 minimal Perl system
ii perl-modules-5.28 5.28.1-6+deb10u1 all Core Perl modules
ii procps 2:3.3.15-2 amd64 /proc file system utilities
ii publicsuffix 20190415.1030-1 all accurate, machine-readable list of domain name suffixes
rc python 2.7.16-1 amd64 interactive high-level object-oriented language (Python2 version)
ii python-minimal 2.7.16-1 amd64 minimal subset of the Python2 language
ii python2 2.7.16-1 amd64 interactive high-level object-oriented language (Python2 version)
ii python2-minimal 2.7.16-1 amd64 minimal subset of the Python2 language
ii python2.7 2.7.16-2+deb10u1 amd64 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.16-2+deb10u1 amd64 Minimal subset of the Python language (version 2.7)
ii python3 3.7.3-1 amd64 interactive high-level object-oriented language (default python3 version)
ii python3-minimal 3.7.3-1 amd64 minimal subset of the Python language (default python3 version)
ii python3.7 3.7.3-2+deb10u2 amd64 Interactive high-level object-oriented language (version 3.7)
ii python3.7-minimal 3.7.3-2+deb10u2 amd64 Minimal subset of the Python language (version 3.7)
ii readline-common 7.0-5 all GNU readline and history libraries, common files
ii rsyslog 8.1901.0-1 amd64 reliable system and kernel logging daemon
ii runc 1.0.0~rc6+dfsg1-3 amd64 Open Container Project - runtime
ii sed 4.7-1 amd64 GNU stream editor for filtering/transforming text
ii sensible-utils 0.0.12 all Utilities for sensible alternative selection
ii ssl-cert 1.0.39 all simple debconf wrapper for OpenSSL
ii sudo 1.8.27-1+deb10u3 amd64 Provide limited super user privileges to specific users
ii systemd 241-7~deb10u6 amd64 system and service manager
ii systemd-sysv 241-7~deb10u6 amd64 system and service manager - SysV links
ii sysvinit-utils 2.93-8 amd64 System-V-like utilities
ii tar 1.30+dfsg-6 amd64 GNU version of the tar archiving utility
ii tasksel 3.53 all tool for selecting tasks for installation on Debian systems
```

```
ii tasksel-data 3.53 all official tasks used for installation of Debian systems
ii tini 0.18.0-1 amd64 tiny but valid init for containers
ii tzdata 2021a-0+deb10u1 all time zone and daylight-saving time data
ii ucf 3.0038+nmu1 all Update Configuration File(s): preserve user changes to config files
ii udev 241-7~deb10u6 amd64 /dev/ and hotplug management daemon
ii usb.ids 2019.07.27-0+deb10u1 all USB ID Repository
ii usbutils 1:010-3 amd64 Linux USB utilities
ii util-linux 2.33.1-0.1 amd64 miscellaneous system utilities
ii vim-common 2:8.1.0875-5 all Vi IMproved - Common files
ii vim-tiny 2:8.1.0875-5 amd64 Vi IMproved - enhanced vi editor - compact version
ii vsftpd 3.0.3-12 amd64 lightweight, efficient FTP server written for security
ii wget 1.20.1-1.1 amd64 retrieves files from the web
ii whiptail 0.52.20-8 amd64 Displays user-friendly dialog boxes from shell scripts
ii xauth 1:1.0.10-1 amd64 X authentication utility
ii xkb-data 2.26-2 all X Keyboard Extension (XKB) configuration data
ii xxd 2:8.1.0875-5 amd64 tool to make (or reverse) a hex dump
ii xz-utils 5.2.4-1 amd64 XZ-format compression utilities
ii zlib1g 1:1.2.11.dfsg-1 amd64 compression library - runtime
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege -

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User: 'jerry'
Port: 22
Proto: SSH
Method: password


See the output of the following plugin for details :

Plugin ID : 102094
Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided -

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User: 'jerry'
Port: 22
Proto: SSH
Method: password
```

56468 - Time of Last System Startup -

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot system boot 4.19.0-14-amd64 Sat Nov 15 07:35 still running
reboot system boot 4.19.0-14-amd64 Sun Apr 4 06:56 - 07:57 (01:01)
reboot system boot 4.19.0-14-amd64 Thu Mar 11 17:43 - 18:26 (00:42)
reboot system boot 4.19.0-14-amd64 Tue Mar 9 02:36 - 02:52 (00:16)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 16:40 - 16:58 (00:18)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 05:01 - 05:16 (00:15)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 04:34 - 04:57 (00:23)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 02:20 - 03:15 (00:55)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 02:10 - 02:17 (00:07)
reboot system boot 4.19.0-14-amd64 Mon Mar 8 01:22 - 01:34 (00:12)
reboot system boot 4.19.0-14-amd64 Sun Mar 7 20:24 - 00:58 (04:34)

wtmp begins Sun Mar 7 20:24:22 2021
```

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.136.108.33 to 10.136.108.235 :
10.136.108.33
10.136.108.235

Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix) -

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:
- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

Path : /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
Version : 5.2.4
Associated Package : liblzma5 5.2.4-1
Confidence : High
Managed by OS : True
Version Source : Package

Path : /usr/bin/xz
Version : 5.2.4
Associated Package : xz-utils 5.2.4-1
Confidence : High
Managed by OS : True
Version Source : Package
```

110483 - Unix / Linux Running Processes Information -

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.9 103932 10092 ? Ss 07:35 0:01 /sbin/init
root 2 0.0 0.0 0 0 ? S 07:35 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? I< 07:35 0:00 [rcu_gp]
root 4 0.0 0.0 0 0 ? I< 07:35 0:00 [rcu_par_gp]
root 6 0.0 0.0 0 0 ? I< 07:35 0:00 [kworker/0:0H-kblockd]
root 8 0.0 0.0 0 0 ? I< 07:35 0:00 [mm_percpu_wq]
root 9 0.7 0.0 0 0 ? S 07:35 0:30 [ksoftirqd/0]
root 10 0.0 0.0 0 0 ? I 07:35 0:02 [rcu_sched]
root 11 0.0 0.0 0 0 ? I 07:35 0:00 [rcu_bh]
root 12 0.0 0.0 0 0 ? S 07:35 0:00 [migration/0]
root 14 0.0 0.0 0 0 ? S 07:35 0:00 [cpuhp/0]
root 15 0.0 0.0 0 0 ? S 07:35 0:00 [kdevtmpfs]
root 16 0.0 0.0 0 0 ? I< 07:35 0:00 [netns]
root 17 0.0 0.0 0 0 ? S 07:35 0:00 [kauditd]
root 18 0.0 0.0 0 0 ? S 07:35 0:00 [khungtaskd]
root 19 0.0 0.0 0 0 ? S 07:35 0:00 [oom_reaper]
root 20 0.0 0.0 0 0 ? I< 07:35 0:00 [writeback]
root 21 0.0 0.0 0 0 ? S 07:35 0:00 [kcompactd0]
root 22 0.0 0.0 0 0 ? SN 07:35 0:00 [ksmd]
root 23 0.0 0.0 0 0 ? SN 07:35 0:00 [khugepaged]
```

```
root 24 0.0 0.0 0 0 ? I< 07:35 0:00 [crypto]
root 25 0.0 0.0 0 0 ? I< 07:35 0:00 [kintegrityd]
root 26 0.0 0.0 0 0 ? I< 07:35 0:00 [kblockd]
root 27 0.0 0.0 0 0 ? I< 07:35 0:00 [edac-poller]
root 28 0.0 0.0 0 0 ? I< 07:35 0:00 [devfreq_wq]
root 29 0.0 0.0 0 0 ? S 07:35 0:00 [watchdogd]
root 32 0.0 0.0 0 0 ? S 07:35 0:00 [kswapd0]
root 50 0.0 0.0 0 0 ? I< 07:35 0:00 [kthrotld]
root 51 0.0 0.0 0 0 ? I< 07:35 0:00 [ipv6_addrconf]
root 52 0.0 0.0 0 0 ? I 07:35 0:00 [kworker/u2:1-events_unbound]
root 61 0.0 0.0 0 0 ? I< 07:35 0:00 [kstrp]
root 108 0.0 0.0 0 0 ? I< 07:35 0:00 [ata_sff]
root 110 0.0 0.0 0 0 ? S 07:35 0:00 [scsi_eh_0]
root 111 0.0 0.0 0 0 ? I< 07:35 0:00 [scsi_tmf_0]
root 112 0.0 0.0 0 0 ? S 07:35 0:00 [scsi_eh_1]
root 114 0.0 0.0 0 0 ? I< 07:35 0:00 [scsi_tmf_1]
root 119 0.0 0.0 0 0 ? S 07:35 0:00 [scsi_eh_2]
root 121 0.0 0.0 0 0 ? I< 07:35 0:00 [scsi_tmf_2]
root 154 0.0 0.0 0 0 ? I< 07:35 0:01 [kworker/0:1H-kblockd]
root 163 0.0 0.0 0 0 ? I< 07:35 0:00 [kdmflush]
root 169 0.0 0.0 0 0 ? I< 07:35 0:00 [kdmflush]
root 196 0.0 0.0 0 0 ? I< 07:35 0:00 [kworker/u3:0]
root 198 0.0 0.0 0 0 ? S 07:35 0:00 [jbd2/dm-0-8]
root 199 0.0 0.0 0 0 ? I< 07:35 0:00 [ext4-rsv-conver]
root 231 0.0 0.8 40516 8724 ? Ss 07:35 0:00 /lib/systemd/systemd-journald
root 252 0.0 0.4 21928 4996 ? Ss 07:35 0:00 /lib/systemd/systemd-udevd
root 299 0.0 0.0 0 0 ? I< 07:35 0:00 [ext4-rsv-conver]
systemd+ 308 0.0 0.6 93084 6364 ? Ssl 07:35 0:00 /lib/systemd/systemd-timesyncd
root 311 0.0 0.0 0 0 ? I< 07:35 0:00 [ttm_swap]
root 312 0.0 0.0 0 0 ? S 07:35 0:00 [irq/18-vmwgfx]
message+ 329 0.0 0.4 8828 4216 ? Ss 07:35 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
activation --syslog-only
root 330 0.0 0.2 8476 2624 ? Ss 07:35 0:00 /usr/sbin/cron -f
root 331 0.0 0.7 225824 7976 ? Ssl 07:35 0:00 /usr/sbin/rsyslogd -n -iNONE
root 332 0.0 0.7 19524 7236 ? Ss 07:35 0:00 /lib/systemd/systemd-logind
root 339 0.1 8.2 795496 83784 ? Ssl 07:35 0:06 /usr/sbin/dockerd -H fd://
root 360 0.0 0.2 6620 3032 ? Ss 07:35 0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root 361 0.0 0.1 5612 1492 tty1 Ss+ 07:35 0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root 363 0.0 0.5 9488 5568 ? Ss 07:35 0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf
/var/lib/dhcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3
root 369 0.0 0.7 15852 7188 ? Ss 07:35 0:00 /usr/sbin/sshd -D
root 414 0.0 0.4 8428 4156 ? Ss 07:35 0:00 /usr/sbin/apache2 -k start
www-data 423 3.9 1.2 755712 12980 ? Sl 07:35 2:41 /usr/sbin/apache2 -k start
www-data 424 4.7 0.8 755884 8932 ? Sl 07:35 3:15 /usr/sbin/apache2 -k start
root 532 0.0 3.1 730720 32220 ? Ssl 07:35 0:03 docker-containerd --config /var/run/docker/containerd/containerd.toml --log-level
info
root 876 0.0 0.0 0 0 ? I 08:24 0:00 [kworker/u2:0-events_unbound]
root 1097 0.0 0.0 0 0 ? I 08:32 0:00 [kworker/0:2-cgroup_destroy]
root 1118 0.1 0.0 0 0 ? I 08:37 0:00 [kworker/0:1-events_power_efficient]
www-data 1119 0.7 1.2 755756 12872 ? Sl 08:39 0:01 /usr/sbin/apache2 -k start
root 1255 0.0 0.0 0 0 ? I 08:42 0:00 [kworker/0:0-memcg_kmem_cache]
jerry 1259 0.0 0.8 21028 8332 ? Ss 08:43 0:00 /lib/systemd/systemd --user
jerry 1260 0.0 0.2 104836 2372 ? S 08:43 0:00 (sd-pam)
root 1315 0.0 0.7 16632 7700 ? Ss 08:43 0:00 sshd: jerry [priv]
jerry 1321 0.0 0.4 16804 4876 ? S 08:43 0:00 sshd: jerry
root 1346 0.2 0.6 19120 6336 ? Ss 08:43 0:00 /lib/systemd/systemd-timedated
root 1856 0.0 0.7 16632 7924 ? Ss 08:43 0:00 sshd: jerry [priv]
jerry 1870 0.0 0.5 16804 5576 ? S 08:43 0:00 sshd: jerry@notty
jerry 1871 0.0 0.3 6644 3276 ? Ss 08:43 0:00 bash -c /bin/ps auxww 2>/dev/null
jerry 1872 0.0 0.3 10632 3244 ? R 08:43 0:00 /bin/ps auxww
root 1878 0.0 0.7 16632 7800 ? Ss 08:43 0:00 sshd: jerry [priv]
root 1884 0.0 0.6 15852 6724 ? Ss 08:43 0:00 sshd: [accepted]
sshd 1886 0.0 0.2 15852 2672 ? S 08:43 0:00 sshd: [net]
jerry 1891 0.0 0.5 16804 5208 ? S 08:43 0:00 sshd: jerry@notty
jerry 1892 0.0 0.3 6644 3192 ? Ss 08:43 0:00 bash -c /bin/df -h 2>/dev/null
jerry 1893 0.0 0.0 6644 236 ? D 08:43 0:00 bash -c /bin/df -h 2>/dev/null
```

152743 - Unix Software Discovery Commands Not Available -

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.
Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,
* Failed privilege escalation,
* Intermittent network disruption, or
* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

unzip -v :
bash: unzip: command not found


Account : jerry
Protocol : SSH
```

189731 - Vim Installed (Linux) -

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/vim.tiny
Version : 8.1
```

182848 - libcurl Installed (Linux / Unix) -

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

Path : /usr/lib/x86_64-linux-gnu/libcurl.so.4.5.0
Version : 7.64.0
Associated Package : libcurl4 7.64.0-4
Managed by OS : True

Path : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.5.0
Version : 7.64.0
Associated Package : libcurl3-gnutls 7.64.0-4
Managed by OS : True
```

52703 - vsftpd Detection -

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source : 220 (vsFTPd 3.0.3)
Version : 3.0.3
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 98% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Debian dla-3588 : vim - security update: Upgrade the vim packages.	58	1
Debian DSA-5096-1 : linux - security update: Upgrade the linux packages.	52	1
Debian dla-3763 : curl - security update: Upgrade the curl packages.	32	1
Debian dla-3818 : apache2 - security update: Upgrade the apache2 packages.	23	1
Debian dla-3850 : glibc-doc - security update: Upgrade the glibc-doc packages.	19	1
Debian dla-3783 : expat - security update: Upgrade the expat packages.	18	1
Debian dla-3844 : git - security update: Upgrade the git packages.	18	1
Debian dla-3771 : idle-python2.7 - security update: Upgrade the idle-python2.7 packages.	17	1
Debian dla-3772 : idle-python3.7 - security update: Upgrade the idle-python3.7 packages.	15	1
Debian dla-3816 : bind9 - security update: Upgrade the bind9 packages.	14	1
Debian dla-3530 : libssl-dev - security update: Upgrade the libssl-dev packages.	11	1
Debian dla-3757 : libnss3 - security update: Upgrade the libnss3 packages.	11	1
Debian dla-3735 : golang-github-opencontainers-runc-dev - security update: Upgrade the golang-github-opencontainers-runc-dev packages.	7	1
Debian DSA-5169-1 : openssl - security update: Upgrade the openssl packages. For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u3.	6	1
Debian dla-3405 : libxml2 - security update: Upgrade the libxml2 packages.	5	1
Debian dla-3732 : sudo - security update: Upgrade the sudo packages.	5	1
Debian dla-3740 : gnutls-bin - security update: Upgrade the gnutls-bin packages.	5	1
Debian DSA-4875-1 : openssl - security update: Upgrade the openssl packages. For the stable distribution (buster), this problem has been fixed in version 1.1.1d-0+deb10u6.	4	1
Debian dla-3602 : libx11-6 - security update: Upgrade the libx11-6 packages.	4	1
Debian dla-3605 : grub-common - security update: Upgrade the grub-common packages.	4	1

Debian dla-3628 : dbus - security update: Upgrade the dbus packages.	4	1
Debian dla-3682 : lib32ncurses-dev - security update: Upgrade the lib32ncurses-dev packages.	4	1
Debian dla-3694 : openssh-client - security update: Upgrade the openssh-client packages.	4	1
Debian dla-3107 : lemon - security update: Upgrade the lemon packages.	3	1
Debian dla-3363 : libpcre2-16-0 - security update: Upgrade the libpcre2-16-0 packages.	3	1
Debian dla-3474 : libnss-myhostname - security update: Upgrade the libnss-myhostname packages.	3	1
Debian dla-3559 : libssh2-1 - security update: Upgrade the libssh2-1 packages.	3	1
Debian dla-3626 : krb5-admin-server - security update: Upgrade the krb5-admin-server packages.	3	1
Debian dla-3804 : libnghttp2-14 - security update: Upgrade the libnghttp2-14 packages.	3	1
Debian DSA-4933-1 : nettle - security update: Upgrade the nettle packages. For the stable distribution (buster), these problems have been fixed in version 3.4.1-1+deb10u1.	2	1
Debian dla-3103 : lib32z1 - security update: Upgrade the lib32z1 packages.	2	1
Debian dla-3146 : isc-dhcp-client - security update: Upgrade the isc-dhcp-client packages.	2	1
Debian dla-3445 : cpio - security update: Upgrade the cpio packages.	2	1
Debian dla-3782 : bsdutils - security update: Upgrade the bsdutils packages.	2	1
Debian dla-3823 : less - security update: Upgrade the less packages.	2	1
Debian DSA-4919-1 : lz4 - security update: Upgrade the lz4 packages. For the stable distribution (buster), this problem has been fixed in version 1.8.3-1+deb10u1.	1	1
Debian DSA-4920-1 : libx11 - security update: Upgrade the libx11 packages. For the stable distribution (buster), this problem has been fixed in version 2:1.6.7-1+deb10u2.	1	1
Debian DSA-5014-1 : icu - security update: Upgrade the icu packages.	1	1
Debian DSA-5087-1 : cyrus-sasl2 - security update: Upgrade the cyrus-sasl2 packages. For the stable distribution (bullseye), this problem has been fixed in version 2.1.27+dfsg-2.1+deb11u1.	1	1
Debian DSA-5122-1 : gzip - security update: Upgrade the gzip packages. For the stable distribution (bullseye), this problem has been fixed in version 1.10-4+deb11u1.	1	1
Debian DSA-5123-1 : xz-utils - security update: Upgrade the xz-utils packages. For the stable distribution (bullseye), this problem has been fixed in version 5.2.5-2.1~deb11u1.	1	1
Debian DSA-5137-1 : needrestart - security update: Upgrade the needrestart packages. For the stable distribution (bullseye), this problem has been fixed in version 3.5-4+deb11u1.	1	1
Debian DSA-5140-1 : openldap - security update: Upgrade the openldap packages. For the stable distribution (bullseye), this problem has been fixed in version 2.4.57+dfsg-3+deb11u1.	1	1
Debian DSA-5147-1 : dpkg - security update: Upgrade the dpkg packages. For the stable distribution (bullseye), this problem has been fixed in version 1.20.10.	1	1
Debian DSA-5150-1 : rsyslog - security update: Upgrade the rsyslog packages. For the stable distribution (bullseye), this problem has been fixed in version 8.2102.0-2+deb11u1.	1	1
Debian DSA-5174-1 : gnupg2 - security update: Upgrade the gnupg2 packages. For the stable distribution (bullseye), this problem has been fixed in version 2.2.27-2+deb11u2.	1	1
Debian dla-3263 : libtasn1-6 - security update: Upgrade the libtasn1-6 packages.	1	1
Debian dla-3332 : libaprutil1 - security update: Upgrade the libaprutil1 packages.	1	1
Debian dla-3461 : libfastjson-dev - security update: Upgrade the libfastjson-dev packages.	1	1
Debian dla-3579 : elfutils - security update: Upgrade the elfutils packages.	1	1
Debian dla-3755 : tar - security update: Upgrade the tar packages.	1	1

Debian dla-3831 : nano - security update: Upgrade the nano packages.	1	1
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795): Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.	1	1