tenable Nessus

Report generated by Tenable Nessus™

Death Note

Sun, 09 Nov 2025 16:52:33 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.255.112.115

CRITICAL	HIGH	MEDIUM	LOW	INFO
11	69	70	4	0

Scan Information

Start time:	Sun Nov 9 16:45:23 2025
End time:	Sun Nov 9 16:52:32 2025

Host Information

IP:	10.255.112.115
MAC Address:	08:00:27:FA:07:43
OS:	Linux Kernel 4.19.0-17-amd64 on Debian 10.10

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+deb10u6
Should be : libssl1.1_1.1.1n-0+deb10u2
Remote package installed : openssl_1.1.1d-0+deb10u6
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+deb10u6
Should be : libssl1.1_1.1.1n-0+deb10u3
Remote package installed : openssl_1.1.1d-0+deb10u6
Should be : openssl_1.1.1n-0+deb10u3
```

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+deb10u3
Should be : libpython3.7-minimal_3.7.3-2+deb10u4
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u3
Should be : libpython3.7-stdlib_3.7.3-2+deb10u4
Remote package installed : python3.7_3.7.3-2+deb10u3
Should be : python3.7_3.7.3-2+deb10u4
Remote package installed : python3.7-minimal_3.7.3-2+deb10u3
Should be : python3.7-minimal_3.7.3-2+deb10u4
```

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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u6
Remote package installed : libcurl4_7.64.0-4+deb10u2
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+deb10u5
Should be : apache2_2.4.38-3+deb10u10
Remote package installed : apache2-bin_2.4.38-3+deb10u5
Should be : apache2-bin_2.4.38-3+deb10u10
Remote package installed : apache2-data_2.4.38-3+deb10u5
Should be : apache2-data_2.4.38-3+deb10u10
Remote package installed : apache2-doc_2.4.38-3+deb10u5
Should be : apache2-doc_2.4.38-3+deb10u10
Remote package installed : apache2-utils_2.4.38-3+deb10u5
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
```

180518 - Debian dla-3555 : libapache2-mod-php7.3 - 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-3555 advisory.

---------- Debian LTS Advisory DLA-3555-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin September 05, 2023 https://wiki.debian.org/LTS

Package : php7.3 Version : 7.3.31-1~deb10u5 CVE ID : CVE-2023-3823 CVE-2023-3824

Security issues were found in PHP, a widely-used open source general purpose scripting language, which could result in information disclosure, denial of service or potentially remote code execution.

CVE-2023-3823

Various XML functions rely on libxml global state to track configuration variables, like whether external entities are loaded.
This state is assumed to be unchanged unless the user explicitly changes it by calling appropriate function. Joas Schilling and Baptista Katapi discovered that, since the state is process-global, other modules such as ImageMagick may also use this library within the same process and change that global state for their internal purposes, and leave it in a state where external entities loading is enabled. This can lead to the situation where external XML is parsed with external entities loaded, which can lead to disclosure of any local files accessible to PHP. This vulnerable state may persist in the same process across many requests, until the process is shut down.

CVE-2023-3824

Niels Dossche discovered that when loading a Phar file, while reading PHAR directory entries, insufficient length checking may lead to a stack buffer overflow, leading potentially to memory corruption or RCE.

For Debian 10 buster, these problems have been fixed in version 7.3.31-1~deb10u5.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2023-3823
https://security-tracker.debian.org/tracker/CVE-2023-3824
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 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-2023-3823
CVE	CVE-2023-3824

Plugin Information

Published: 2023/09/06, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
Should be : libapache2-mod-php7.3_7.3.31-1~deb10u5
Remote package installed : php7.3_7.3.29-1~deb10u1
Should be : php7.3_7.3.31-1~deb10u5
Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
Should be : php7.3-cgi_7.3.31-1~deb10u5
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u5
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u5
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u5
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u5
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u5
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u5
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u5
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u5
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u5
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u5
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u5
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u5
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u5
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u5
```

181562 - Debian dla-3570 : libwebp-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-3570 advisory.

- ---------- Debian LTS Advisory DLA-3570-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 18, 2023 https://wiki.debian.org/LTS
- ----------

Package : libwebp Version : 0.6.1-2+deb10u3 CVE ID : CVE-2023-4863

A buffer overflow in parsing WebP images may result in the execution of arbitrary code.

For Debian 10 buster, this problem has been fixed in version 0.6.1-2+deb10u3.

We recommend that you upgrade your libwebp packages.

For the detailed security status of libwebp please refer to its security tracker page at:

https://security-tracker.debian.org/tracker/libwebp

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/libwebp
https://security-tracker.debian.org/tracker/CVE-2023-4863
https://packages.debian.org/source/buster/libwebp

Solution

Upgrade the libwebp-dev 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

8.4 (CVSS:3.0/E:H/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

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

References

CVE	CVE-2023-4863
XREF	CISA-KNOWN-EXPLOITED:2023/10/04

Plugin Information

Published: 2023/09/18, Modified: 2025/01/23

Plugin Output

tcp/0

```
Remote package installed : libwebp6_0.6.1-2+deb10u1
Should be : libwebp6_0.6.1-2+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+deb10u3
Should be : libpython3.7-minimal_3.7.3-2+deb10u6
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u3
Should be : libpython3.7-stdlib_3.7.3-2+deb10u6
Remote package installed : python3.7_3.7.3-2+deb10u3
Should be : python3.7_3.7.3-2+deb10u6
Remote package installed : python3.7-minimal_3.7.3-2+deb10u3
Should be : python3.7-minimal_3.7.3-2+deb10u6
```

152271 - Debian DSA-4951-1 : bluez - 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-4951 advisory.

Several vulnerabilities were discovered in Bluez, the Linux Bluetooth protocol stack. CVE-2020-26558 / CVE-2021-0129 It was discovered that Bluez does not properly check permissions during pairing operation, which could allow an attacker to impersonate the initiating device. CVE-2020-27153 Jay LV discovered a double free flaw in the disconnect_cb() routine in the gattool. A remote attacker can take advantage of this flaw during service discovery for denial of service, or potentially, execution of arbitrary code. For the stable distribution (buster), these problems have been fixed in version 5.50-1.2~deb10u2. We recommend that you upgrade your bluez packages. For the detailed security status of bluez please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bluez

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=989614
https://security-tracker.debian.org/tracker/source-package/bluez
https://www.debian.org/security/2021/dsa-4951
https://security-tracker.debian.org/tracker/CVE-2020-26558
https://security-tracker.debian.org/tracker/CVE-2020-27153
https://security-tracker.debian.org/tracker/CVE-2021-0129
https://packages.debian.org/source/buster/bluez

Solution

Upgrade the bluez packages.

For the stable distribution (buster), these problems have been fixed in version 5.50-1.2~deb10u2.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (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-2020-26558
CVE	CVE-2020-27153
CVE	CVE-2021-0129

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : bluetooth_5.50-1.2~deb10u1
Should be : bluetooth_5.50-1.2~deb10u2
Remote package installed : bluez_5.50-1.2~deb10u1
Should be : bluez_5.50-1.2~deb10u2
```

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+deb10u6
Should be : libssl1.1_1.1.1d-0+deb10u7
Remote package installed : openssl_1.1.1d-0+deb10u6
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+deb10u5
Should be : apache2_2.4.38-3+deb10u6
Remote package installed : apache2-bin_2.4.38-3+deb10u5
Should be : apache2-bin_2.4.38-3+deb10u6
Remote package installed : apache2-data_2.4.38-3+deb10u5
Should be : apache2-data_2.4.38-3+deb10u6
Remote package installed : apache2-doc_2.4.38-3+deb10u5
Should be : apache2-doc_2.4.38-3+deb10u6
Remote package installed : apache2-utils_2.4.38-3+deb10u5
Should be : apache2-utils_2.4.38-3+deb10u6
```

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+deb10u5
Should be : apache2_2.4.38-3+deb10u7
Remote package installed : apache2-bin_2.4.38-3+deb10u5
Should be : apache2-bin_2.4.38-3+deb10u7
Remote package installed : apache2-data_2.4.38-3+deb10u5
Should be : apache2-data_2.4.38-3+deb10u7
Remote package installed : apache2-doc_2.4.38-3+deb10u5
Should be : apache2-doc_2.4.38-3+deb10u7
Remote package installed : apache2-utils_2.4.38-3+deb10u5
Should be : apache2-utils_2.4.38-3+deb10u7
```

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-4.19.0-17-amd64_4.19.194-2
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+deb10u7
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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u8
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_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
```

166732 - Debian dla-3171 : distro-info-data - 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-3171 advisory.

---------- Debian LTS Advisory DLA-3171-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Stefano Rivera October 30, 2022 https://wiki.debian.org/LTS

Package : distro-info-data Version : 0.41+deb10u6

This is a routine update of the distro-info-data database for Debian LTS users.

It includes a correction to some historical data, and adds Ubuntu 23.04, Lunar Lobster.

For Debian 10 buster, these issues have been fixed in version 0.41+deb10u6.

We recommend that you upgrade your distro-info-data packages.

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

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?9851c5ba
https://packages.debian.org/source/buster/distro-info-data

Solution

Upgrade the distro-info-data packages.

For Debian 10 buster, these issues have been fixed in version 0.41+deb10u6.

Risk Factor

High

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : distro-info-data_0.41+deb10u3
Should be : distro-info-data_0.41+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+deb10u2
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+deb10u7
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+deb10u1
Should be : isc-dhcp-client_4.4.1-2+deb10u3
Remote package installed : isc-dhcp-common_4.4.1-2+deb10u1
Should be : isc-dhcp-common_4.4.1-2+deb10u3
```

171861 - Debian dla-3337 : libmariadb-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-3337 advisory.

- ---------- Debian LTS Advisory DLA-3337-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Otto Keklinen February 23, 2023 https://wiki.debian.org/LTS
- ----------

Package : mariadb-10.3 Version : 1:10.3.38-0+deb10u1 Debian Bug : 1008629

A new MariaDB minor maintenance release 10.3.38 has been released. It includes fix for a major performance/memory consumption issue (MDEV-29988).

For further details, see the MariaDB 10.3 release notes:

https://mariadb.com/kb/en/mariadb-10-3-37-release-notes/ https://mariadb.com/kb/en/mariadb-10-3-38-release-notes/

For Debian 10 buster, this problem has been fixed in version 1:10.3.38-0+deb10u1.

We recommend that you upgrade your mariadb-10.3 packages.

For the detailed security status of mariadb-10.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.3

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

http://www.nessus.org/u?cb6537b5
https://packages.debian.org/source/buster/mariadb-10.3

Solution

Upgrade the libmariadb-dev packages.

Risk Factor

High

Plugin Information

Published: 2023/02/23, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libmariadb3_1:10.3.29-0+deb10u1
Should be : libmariadb3_1:10.3.38-0+deb10u1
Remote package installed : mariadb-client_1:10.3.29-0+deb10u1
Should be : mariadb-client_1:10.3.38-0+deb10u1
Remote package installed : mariadb-client-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-10.3_1:10.3.38-0+deb10u1
Remote package installed : mariadb-client-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-core-10.3_1:10.3.38-0+deb10u1
Remote package installed : mariadb-common_1:10.3.29-0+deb10u1
Should be : mariadb-common_1:10.3.38-0+deb10u1
Remote package installed : mariadb-server_1:10.3.29-0+deb10u1
Should be : mariadb-server_1:10.3.38-0+deb10u1
Remote package installed : mariadb-server-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-10.3_1:10.3.38-0+deb10u1
Remote package installed : mariadb-server-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-core-10.3_1:10.3.38-0+deb10u1
```

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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u5
Remote package installed : libcurl4_7.64.0-4+deb10u2
Should be : libcurl4_7.64.0-4+deb10u5
```

171925 - Debian dla-3345 : libapache2-mod-php7.3 - 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-3345 advisory.

---------- Debian LTS Advisory DLA-3345-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin February 26, 2023 https://wiki.debian.org/LTS

Package : php7.3 Version : 7.3.31-1~deb10u3 CVE ID : CVE-2022-31631 CVE-2023-0567 CVE-2023-0568 CVE-2023-0662 Debian Bug : 1031368

Multiple security issues were found in PHP, a widely-used open source general purpose scripting language, which could result in denial of service or incorrect validation of BCrypt hashes.

CVE-2022-31631

Due to an uncaught integer overflow, `PDO::quote()` of PDO_SQLite may return an improperly quoted string. The exact details likely depend on the implementation of `sqlite3_snprintf()`, but with some versions it is possible to force the function to return a single apostrophe, if the function is called on user supplied input without any length restrictions in place.

CVE-2023-0567

Tim Dsterhus discovered that malformed BCrypt hashes that include a `$` within their salt part trigger a buffer overread and may erroneously validate any password as valid. (`Password_verify()` always return `true` with such inputs.)

CVE-2023-0568

1-byte array overrun when appending slash to paths during path resolution.

CVE-2023-0662

Jakob Ackermann discovered a Denial of Service vulnerability when parsing multipart request body: the request body parsing in PHP allows any unauthenticated attacker to consume a large amount of CPU time and trigger excessive logging.

For Debian 10 buster, these problems have been fixed in version 7.3.31-1~deb10u3.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2022-31631
https://security-tracker.debian.org/tracker/CVE-2023-0567
https://security-tracker.debian.org/tracker/CVE-2023-0568
https://security-tracker.debian.org/tracker/CVE-2023-0662
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 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

7.3 (CVSS:3.0/E:P/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

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

STIG Severity

I

References

CVE	CVE-2022-31631
CVE	CVE-2023-0567
CVE	CVE-2023-0568
CVE	CVE-2023-0662
XREF	IAVA:2023-A-0105-S

Plugin Information

Published: 2023/02/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
Should be : libapache2-mod-php7.3_7.3.31-1~deb10u3
Remote package installed : php7.3_7.3.29-1~deb10u1
Should be : php7.3_7.3.31-1~deb10u3
Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
Should be : php7.3-cgi_7.3.31-1~deb10u3
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u3
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u3
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u3
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u3
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u3
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u3
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u3
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u3
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u3
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u3
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u3
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u3
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u3
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u3
```

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+deb10u2
Should be : libxml2_2.9.4+dfsg1-7+deb10u6
```

174968 - Debian dla-3411 : distro-info-data - 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-3411 advisory.

---------- Debian LTS Advisory DLA-3411-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Stefano

Rivera April 30, 2023 https://wiki.debian.org/LTS

Package : distro-info-data Version : 0.41+deb10u7

This is a routine update of the distro-info-data database for Debian LTS users.

It includes the expected release date for Debian 12, adds Debian 14, adds Ubuntu 23.10, and some minor updates to EoL dates for Ubuntu releases.

For Debian 10 buster, these issues have been fixed in version 0.41+deb10u6.

We recommend that you upgrade your distro-info-data packages.

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

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?9851c5ba
https://packages.debian.org/source/buster/distro-info-data

Solution

Upgrade the distro-info-data packages.

Risk Factor

High

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : distro-info-data_0.41+deb10u3
Should be : distro-info-data_0.41+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
```

176521 - Debian dla-3439 : libwebp-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-3439 advisory.

- ---------- Debian LTS Advisory DLA-3439-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb May 31, 2023 https://wiki.debian.org/LTS
- ----------

Package : libwebp Version : 0.6.1-2+deb10u2 CVE ID : CVE-2023-1999 Debian Bug : 1035371

It was discovered that there was a potential arbitrary code execution vulnerability in libwebp, a library to support the WebP image compression format.

For Debian 10 buster, this problem has been fixed in version 0.6.1-2+deb10u2.

We recommend that you upgrade your libwebp packages.

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

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-2023-1999
https://security-tracker.debian.org/tracker/source-package/libwebp
https://packages.debian.org/source/buster/libwebp

Solution

Upgrade the libwebp-dev 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-2023-1999

Plugin Information

Published: 2023/05/31, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libwebp6_0.6.1-2+deb10u1
Should be : libwebp6_0.6.1-2+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
```

177457 - Debian dla-3459 : libxpm-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-3459 advisory.

- ---------- Debian LTS Advisory DLA-3459-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris June 20, 2023 https://wiki.debian.org/LTS
- ----------

Package : libxpm Version : 1:3.5.12-1+deb10u1 CVE ID : CVE-2022-4883 CVE-2022-44617 CVE-2022-46285

libxpm is a library handling X PixMap image format (so called xpm files).
xpm files are an extension of the monochrome X BitMap format specified in the X protocol, and is commonly used in traditional X applications.

CVE-2022-4883

When processing files with .Z or .gz extensions, the library calls external programs to compress and uncompress files, relying on the PATH environment variable to find these programs, which could allow a malicious user to execute other programs by manipulating the PATH environment variable.

CVE-2022-44617

When processing a file with width of 0 and a very large height, some parser functions will be called repeatedly and can lead to an infinite loop, resulting in a Denial of Service in the application linked to the library.

CVE-2022-46285

When parsing a file with a comment not closed, an end-of-file condition will not be detected, leading to an infinite loop and resulting in a Denial of Service in the application linked to the library.

For Debian 10 buster, these problems have been fixed in version 1:3.5.12-1+deb10u1.

We recommend that you upgrade your libxpm packages.

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

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/libxpm
https://security-tracker.debian.org/tracker/CVE-2022-44617
https://security-tracker.debian.org/tracker/CVE-2022-46285
https://security-tracker.debian.org/tracker/CVE-2022-4883
https://packages.debian.org/source/buster/libxpm

Solution

Upgrade the libxpm-dev 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-2022-4883
CVE	CVE-2022-44617
CVE	CVE-2022-46285

Plugin Information

Published: 2023/06/20, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libxpm4_1:3.5.12-1
Should be : libxpm4_1:3.5.12-1+deb10u1
```

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+deb10u2
Should be : libx11-6_2:1.6.7-1+deb10u3
Remote package installed : libx11-data_2:1.6.7-1+deb10u2
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+deb10u3
Should be : libpython3.7-minimal_3.7.3-2+deb10u5
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u3
Should be : libpython3.7-stdlib_3.7.3-2+deb10u5
Remote package installed : python3.7_3.7.3-2+deb10u3
Should be : python3.7_3.7.3-2+deb10u5
Remote package installed : python3.7-minimal_3.7.3-2+deb10u3
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+deb10u1
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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u9
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u9
```

179135 - Debian dla-3513 : libtiff-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-3513 advisory.

- ---------- Debian LTS Advisory DLA-3513-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Adrian Bunk July 31, 2023 https://wiki.debian.org/LTS
- ----------

Package : tiff Version : 4.1.0+git191117-2~deb10u8 CVE ID : CVE-2023-2908 CVE-2023-3316 CVE-2023-3618 CVE-2023-25433 CVE-2023-26965 CVE-2023-26966 CVE-2023-38288 CVE-2023-38289 Debian Bug : 1040945

Multiple vulnerabilities were found in tiff, a library and tools providing support for the Tag Image File Format (TIFF).

CVE-2023-2908

NULL pointer dereference in tif_dir.c

CVE-2023-3316

NULL pointer dereference in TIFFClose()

CVE-2023-3618

Buffer overflow in tiffcrop

CVE-2023-25433

Buffer overflow in tiffcrop

CVE-2023-26965

Use after free in tiffcrop

CVE-2023-26966

Buffer overflow in uv_encode()

CVE-2023-38288

Integer overflow in tiffcp

CVE-2023-38289

Integer overflow in raw2tiff

For Debian 10 buster, these problems have been fixed in version 4.1.0+git191117-2~deb10u8.

We recommend that you upgrade your tiff packages.

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

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/tiff
https://security-tracker.debian.org/tracker/CVE-2023-25433
https://security-tracker.debian.org/tracker/CVE-2023-26965
https://security-tracker.debian.org/tracker/CVE-2023-26966
https://security-tracker.debian.org/tracker/CVE-2023-2908
https://security-tracker.debian.org/tracker/CVE-2023-3316
https://security-tracker.debian.org/tracker/CVE-2023-3618
https://security-tracker.debian.org/tracker/CVE-2023-38288
https://security-tracker.debian.org/tracker/CVE-2023-38289
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the libtiff-dev 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-2023-2908
CVE	CVE-2023-3316

CVE	CVE-2023-3618
CVE	CVE-2023-25433
CVE	CVE-2023-26965
CVE	CVE-2023-26966
CVE	CVE-2023-38288
CVE	CVE-2023-38289

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u8
```

181858 - Debian dla-3583 : libglib2.0-0 - 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-3583 advisory.

---------- Debian LTS Advisory DLA-3583-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Santiago Ruano Rincn September 25, 2023 https://wiki.debian.org/LTS

Package : glib2.0 Version : 2.58.3-2+deb10u5 CVE ID : CVE-2023-29499 CVE-2023-32611 CVE-2023-32665

Several security vulnerabilities were found in GLib, a general-purpose utility library, used by projects such as GTK+, GIMP, and GNOME.

CVE-2023-29499

GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service.

CVE-2023-32611

GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service.

CVE-2023-32665

GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service.

For Debian 10 buster, these problems have been fixed in version 2.58.3-2+deb10u5.

We recommend that you upgrade your glib2.0 packages.

For the detailed security status of glib2.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glib2.0

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/glib2.0
https://security-tracker.debian.org/tracker/CVE-2023-29499
https://security-tracker.debian.org/tracker/CVE-2023-32611
https://security-tracker.debian.org/tracker/CVE-2023-32665
https://packages.debian.org/source/buster/glib2.0

Solution

Upgrade the libglib2.0-0 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-2023-29499
CVE	CVE-2023-32611
CVE	CVE-2023-32665

Plugin Information

Published: 2023/09/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.58.3-2+deb10u3
Should be : libglib2.0-0_2.58.3-2+deb10u5
Remote package installed : libglib2.0-data_2.58.3-2+deb10u3
Should be : libglib2.0-data_2.58.3-2+deb10u5
```

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
```

184024 - Debian dla-3639 : distro-info-data - 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-3639 advisory.

---------- Debian LTS Advisory DLA-3639-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Stefano Rivera October 30, 2023 https://wiki.debian.org/LTS

Package : distro-info-data Version : 0.41+deb10u8

This is a routine update of the distro-info-data database for Debian LTS users.

It includes Ubuntu 24.10, and makes some minor updates to older EoL dates.

For Debian 10 buster, this problem has been fixed in version 0.41+deb10u8.

We recommend that you upgrade your distro-info-data packages.

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

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?9851c5ba
https://packages.debian.org/source/buster/distro-info-data

Solution

Upgrade the distro-info-data packages.

Risk Factor

High

Plugin Information

Published: 2023/10/30, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : distro-info-data_0.41+deb10u3
Should be : distro-info-data_0.41+deb10u8
```

186288 - Debian dla-3666 : python3-reportbug - 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-3666 advisory.

- ---------- Debian LTS Advisory DLA-3666-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris November 26, 2023 https://wiki.debian.org/LTS
- ----------

Package : reportbug Version : 7.5.3~deb10u2

Python version reported by reportbug, a debian tool for bug reporting was incorrect (not PEP440 compliant) and may break unreleated software like pip, a python package manager, used for local development of python packages.

For Debian 10 buster, this problem has been fixed in version 7.5.3~deb10u2.

We recommend that you upgrade your reportbug packages.

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

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/reportbug
https://packages.debian.org/source/buster/reportbug

Solution

Upgrade the python3-reportbug packages.

Risk Factor

High

Plugin Information

Published: 2023/11/26, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : python3-reportbug_7.5.3~deb10u1
Should be : python3-reportbug_7.5.3~deb10u2
Remote package installed : reportbug_7.5.3~deb10u1
Should be : reportbug_7.5.3~deb10u2
```

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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u10
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u10
```

189916 - Debian dla-3731 : man-db - 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-3731 advisory.

---------- Debian LTS Advisory DLA-3731-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Colin Watson February 01, 2024 https://wiki.debian.org/LTS

Package : man-db Version : 2.8.5-2+deb10u1 CVE ID :
Debian Bug : 926450 948238 1061870

man-db provides the man command used for reading manual pages.

man-db 2.7.6.1-3 added AppArmor confinement for filter programs called by man, and man-db 2.8.0 added a seccomp sandbox to confine subprocesses that handle untrusted data. These hardening measures caused various problems that have been fixed in more recent releases: the AppArmor confinement broke the ability to save compressed cat pages under /var/cache/man/, while the seccomp sandbox broke Hardened Malloc as well as systems using mksh-derived shells.

For Debian 10 buster, these problems have been fixed in version 2.8.5-2+deb10u1.

We recommend that you upgrade your man-db packages.

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

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/man-db
https://packages.debian.org/source/buster/man-db

Solution

Upgrade the man-db packages.

Risk Factor

High

Plugin Information

Published: 2024/02/01, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : man-db_2.8.5-2
Should be : man-db_2.8.5-2+deb10u1
```

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+deb10u7
Should be : libgnutls30_3.6.7-4+deb10u12
```

191058 - Debian dla-3743 : hostapd - 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-3743 advisory.

- ---------- Debian LTS Advisory DLA-3743-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb February 27, 2024 https://wiki.debian.org/LTS
- ----------

Package : wpa Version : 2:2.7+git20190128+0c1e29f-6+deb10u4 CVE ID : CVE-2023-52160 Debian Bug : 1064061

It was discovered that there was a potential authentication bypass vulnerability in wpa, a set of tools including the widely-used wpasupplicant client for authenticating with WPA and WPA2 wireless networks.

For an attack to have been successful, wpasupplicant must have been configured to not verify the network's TLS certificate during Phase 1 of the authentication cycle; a eap_peap_decrypt vulnerability could have been used to skip Phase 2 authentication by sending an EAP-TLV Success packet instead of starting Phase 2.

For Debian 10 buster, this problem has been fixed in version 2:2.7+git20190128+0c1e29f-6+deb10u4.

We recommend that you upgrade your wpa packages.

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

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/wpa
https://security-tracker.debian.org/tracker/CVE-2023-52160
https://packages.debian.org/source/buster/wpa

Solution

Upgrade the hostapd 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:H/I:N/A:N)

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-52160

Plugin Information

Published: 2024/02/27, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : wpasupplicant_2:2.7+git20190128+0c1e29f-6+deb10u3
Should be : wpasupplicant_2:2.7+git20190128+0c1e29f-6+deb10u4
```

191553 - Debian dla-3750 : php-phpseclib - 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-3750 advisory.

---------- Debian LTS Advisory DLA-3750-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin March 05, 2024 https://wiki.debian.org/LTS

Package : php-phpseclib Version : 2.0.30-2~deb10u3 CVE ID : CVE-2024-27354 CVE-2024-27355

Security issues were discovered in php-phpseclib, a PHP library for arbitrary-precision integer arithmetic, which could lead to Denial of Service.

CVE-2024-27354

An attacker can construct a malformed certificate containing an extremely large prime to cause a denial of service (CPU consumption for an `isPrime` primality check).

This issue was introduced when attempting to fix CVE-2023-27560.

CVE-2024-27355

When processing the ASN.1 object identifier of a certificate, a sub identifier may be provided that leads to a denial of service (CPU consumption for `decodeOID`).

For Debian 10 buster, these problems have been fixed in version 2.0.30-2~deb10u3.

We recommend that you upgrade your php-phpseclib packages.

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

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

http://www.nessus.org/u?bb7f1a05
https://security-tracker.debian.org/tracker/CVE-2023-27560
https://security-tracker.debian.org/tracker/CVE-2024-27354
https://security-tracker.debian.org/tracker/CVE-2024-27355
https://packages.debian.org/source/buster/php-phpseclib

Solution

Upgrade the php-phpseclib 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-2023-27560
CVE	CVE-2024-27354
CVE	CVE-2024-27355

Plugin Information

Published: 2024/03/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : php-phpseclib_2.0.14-1
Should be : php-phpseclib_2.0.30-2~deb10u3
```

191791 - Debian dla-3758 : libtiff-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-3758 advisory.

---------- Debian LTS Advisory DLA-3758-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Abhijith PA March 11, 2024 https://wiki.debian.org/LTS

Package : tiff Version : 4.1.0+git191117-2~deb10u9 CVE ID : CVE-2023-3576 CVE-2023-52356

Two vulnerabilities were discovered in tiff, Tag Image File Format library.

CVE-2023-3576

A memory leak flaw was found in Libtiff's tiffcrop utility. This issue occurs when tiffcrop operates on a TIFF image file, allowing an attacker to pass a crafted TIFF image file to tiffcrop utility, which causes this memory leak issue, resulting an application crash, eventually leading to a denial of service

CVE-2023-52356

A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service.

For Debian 10 buster, these problems have been fixed in version 4.1.0+git191117-2~deb10u9.

We recommend that you upgrade your tiff packages.

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

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/tiff
https://security-tracker.debian.org/tracker/CVE-2023-3576
https://security-tracker.debian.org/tracker/CVE-2023-52356
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the libtiff-dev 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-2023-3576
CVE	CVE-2023-52356

Plugin Information

Published: 2024/03/11, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u9
```

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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u9
Remote package installed : libcurl4_7.64.0-4+deb10u2
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+deb10u3
Should be : libpython3.7-minimal_3.7.3-2+deb10u7
Remote package installed : libpython3.7-stdlib_3.7.3-2+deb10u3
Should be : libpython3.7-stdlib_3.7.3-2+deb10u7
Remote package installed : python3.7_3.7.3-2+deb10u3
Should be : python3.7_3.7.3-2+deb10u7
Remote package installed : python3.7-minimal_3.7.3-2+deb10u3
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
```

194891 - Debian dla-3806 : distro-info-data - 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-3806 advisory.

---------- Debian LTS Advisory DLA-3806-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Stefano Rivera May 01, 2024 https://wiki.debian.org/LTS

Package : distro-info-data Version : 0.41+deb10u9

This is a routine update of the distro-info-data database for Debian LTS users.

It adds Ubuntu 24.10.

Also included are LTS and ELTS columns for Debian, and ESM columns for Ubuntu. The version of distro-info in buster is not able to display the data from these columns, but they are present in the CSV.

For Debian 10 buster, this problem has been fixed in version 0.41+deb10u9.

We recommend that you upgrade your distro-info-data packages.

For the detailed security status of distro-info-data please refer to its security tracker page at:

https://security-tracker.debian.org/tracker/distro-info-data

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?9851c5ba
https://packages.debian.org/source/buster/distro-info-data

Solution

Upgrade the distro-info-data packages.

Risk Factor

High

Plugin Information

Published: 2024/05/01, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : distro-info-data_0.41+deb10u3
Should be : distro-info-data_0.41+deb10u9
```

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
```

195146 - Debian dla-3810 : libapache2-mod-php7.3 - 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-3810 advisory.

---------- Debian LTS Advisory DLA-3810-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin May 07, 2024 https://wiki.debian.org/LTS

Package : php7.3 Version : 7.3.31-1~deb10u6 CVE ID : CVE-2024-2756 CVE-2024-3096

Security issues were found in PHP, a widely-used open source general purpose scripting language, which could result in information disclosure or incorrect validation of password hashes.

CVE-2024-2756

Marco Squarcina discovered that network and same-site attackers can set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.

This issue stems from an incomplete fix to CVE-2022-31629.

CVE-2024-3096

Eric Stern discovered that if a password stored with password_hash() starts with a null byte (\x00), testing a blank string as the password via password_verify() incorrectly returns true.

If a user were able to create a password with a leading null byte (unlikely, but syntactically valid), the issue would allow an attacker to trivially compromise the

victim's account by attempting to sign in with a blank string.

For Debian 10 buster, these problems have been fixed in version 7.3.31-1~deb10u6.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2022-31629
https://security-tracker.debian.org/tracker/CVE-2024-2756
https://security-tracker.debian.org/tracker/CVE-2024-3096
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 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:H/A:N)

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:C/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-31629
CVE	CVE-2024-2756
CVE	CVE-2024-3096

Plugin Information

Published: 2024/05/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
  Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
  Should be : libapache2-mod-php7.3_7.3.31-1~deb10u6
  Remote package installed : php7.3_7.3.29-1~deb10u1
  Should be : php7.3_7.3.31-1~deb10u6
  Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
  Should be : php7.3-cgi_7.3.31-1~deb10u6
  Remote package installed : php7.3-cli_7.3.29-1~deb10u1
  Should be : php7.3-cli_7.3.31-1~deb10u6
  Remote package installed : php7.3-common_7.3.29-1~deb10u1
  Should be : php7.3-common_7.3.31-1~deb10u6
  Remote package installed : php7.3-curl_7.3.29-1~deb10u1
  Should be : php7.3-curl_7.3.31-1~deb10u6
  Remote package installed : php7.3-gd_7.3.29-1~deb10u1
  Should be : php7.3-gd_7.3.31-1~deb10u6
  Remote package installed : php7.3-intl_7.3.29-1~deb10u1
  Should be : php7.3-intl_7.3.31-1~deb10u6
  Remote package installed : php7.3-json_7.3.29-1~deb10u1
  Should be : php7.3-json_7.3.31-1~deb10u6
  Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
  Should be : php7.3-mbstring_7.3.31-1~deb10u6
```

```
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u6
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u6
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u6
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u6
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u6
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u6
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u6
```

195178 - Debian dla-3811 : pypy-idna - 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-3811 advisory.

---------- Debian LTS Advisory DLA-3811-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin May 08, 2024 https://wiki.debian.org/LTS

Package : python-idna Version : 2.6-1+deb10u1 CVE ID : CVE-2024-3651 Debian Bug : 1069127

Guido Vranken discovered an issue in python3-idna, a library to support the Internationalized Domain Names in Applications (IDNA) protocol. A specially crafted argument to the idna.encode() function could consume significant resources, which may lead to Denial of Service.

For Debian 10 buster, this problem has been fixed in version 2.6-1+deb10u1.

We recommend that you upgrade your python-idna packages.

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

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/python-idna
https://security-tracker.debian.org/tracker/CVE-2024-3651
https://packages.debian.org/source/buster/python-idna

Solution

Upgrade the pypy-idna 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-2024-3651

Plugin Information

Published: 2024/05/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : python3-idna_2.6-1
Should be : python3-idna_2.6-1+deb10u1
```

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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u11
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u11
```

197925 - Debian dla-3820 : bluetooth - 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-3820 advisory.

- ---------- Debian LTS Advisory DLA-3820-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Arturo Borrero Gonzalez May 25, 2024 https://wiki.debian.org/LTS
- ----------

Package : bluez Version : 5.50-1.2~deb10u5 CVE ID : CVE-2023-27349

An problem has been fixed with the handling of the AVRCP protocol in the bluetooth stack that could lead to remote code execution.

For Debian 10 buster, this problem has been fixed in version 5.50-1.2~deb10u5.

We recommend that you upgrade your bluez packages.

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

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/bluez
https://security-tracker.debian.org/tracker/CVE-2023-27349
https://packages.debian.org/source/buster/bluez

Solution

Upgrade the bluetooth packages.

Risk Factor

High

CVSS v3.0 Base Score

8.0 (CVSS:3.0/AV:A/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:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-27349

Plugin Information

Published: 2024/05/25, Modified: 2025/07/09

Plugin Output

tcp/0

```
Remote package installed : bluetooth_5.50-1.2~deb10u1
Should be : bluetooth_5.50-1.2~deb10u5
Remote package installed : bluez_5.50-1.2~deb10u1
Should be : bluez_5.50-1.2~deb10u5
```

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
```

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 : libnss-systemd_241-7~deb10u7
Should be : libnss-systemd_241-7~deb10u8
Remote package installed : libpam-systemd_241-7~deb10u7
Should be : libpam-systemd_241-7~deb10u8
Remote package installed : libsystemd0_241-7~deb10u7
Should be : libsystemd0_241-7~deb10u8
Remote package installed : libudev1_241-7~deb10u7
Should be : libudev1_241-7~deb10u8
Remote package installed : systemd_241-7~deb10u7
Should be : systemd_241-7~deb10u8
Remote package installed : systemd-sysv_241-7~deb10u7
Should be : systemd-sysv_241-7~deb10u8
Remote package installed : udev_241-7~deb10u7
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
```

154428 - Debian DSA-4993-1 : php7.3 - 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-4993 advisory.

An out-of-bounds read and write flaw was discovered in the PHP-FPM code, which could result in escalation of privileges from local unprivileged user to the root user. For the oldstable distribution (buster), this problem has been fixed in version 7.3.31-1~deb10u1. We recommend that you upgrade your php7.3 packages. For the detailed security status of php7.3 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/php7.3

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/php7.3
https://www.debian.org/security/2021/dsa-4993
https://security-tracker.debian.org/tracker/CVE-2021-21703
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the php7.3 packages.

Risk Factor

Medium

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

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)

STIG Severity

I

References

CVE	CVE-2021-21703
XREF	IAVA:2021-A-0503-S

Plugin Information

Published: 2021/10/26, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
Should be : libapache2-mod-php7.3_7.3.31-1~deb10u1
Remote package installed : php7.3_7.3.29-1~deb10u1
Should be : php7.3_7.3.31-1~deb10u1
Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
Should be : php7.3-cgi_7.3.31-1~deb10u1
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u1
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u1
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u1
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u1
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u1
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u1
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u1
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u1
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u1
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u1
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u1
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u1
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u1
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u1
```

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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u6
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u6
```

154750 - Debian DSA-4997-1 : tiff - 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-4997 advisory.

- Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the TIFFVGetField funtion in the component 'libtiff/tif_dir.c'. (CVE-2020-19143)

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/tiff
https://www.debian.org/security/2021/dsa-4997
https://security-tracker.debian.org/tracker/CVE-2020-19143
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the tiff packages.

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

5.7 (CVSS:3.0/E:U/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

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

References

CVE CVE-2020-19143

Plugin Information

Published: 2021/10/31, Modified: 2021/10/31

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u3
```

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+deb10u6
Should be : libssl1.1_1.1.1d-0+deb10u8
Remote package installed : openssl_1.1.1d-0+deb10u6
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 : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u5
  Should be : bind9-host_1:9.11.5.P4+dfsg-5.1+deb10u7
  Remote package installed : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u5
  Should be : libbind9-161_1:9.11.5.P4+dfsg-5.1+deb10u7
  Remote package installed : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u5
  Should be : libdns-export1104_1:9.11.5.P4+dfsg-5.1+deb10u7
  Remote package installed : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u5
  Should be : libdns1104_1:9.11.5.P4+dfsg-5.1+deb10u7
  Remote package installed : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u5
  Should be : libisc-export1100_1:9.11.5.P4+dfsg-5.1+deb10u7
```

```
Remote package installed : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisc1100_1:9.11.5.P4+dfsg-5.1+deb10u7
Remote package installed : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccc161_1:9.11.5.P4+dfsg-5.1+deb10u7
Remote package installed : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : libisccfg163_1:9.11.5.P4+dfsg-5.1+deb10u7
Remote package installed : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u5
Should be : liblwres161_1:9.11.5.P4+dfsg-5.1+deb10u7
```

159229 - Debian DSA-5108-1 : tiff - 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-5108 advisory.

Multiple vulnerabilities have been discovered in the libtiff library and the included tools, which may result in denial of service if malformed image files are processed. For the oldstable distribution (buster), these problems have been fixed in version 4.1.0+git191117-2~deb10u4. For the stable distribution (bullseye), these problems have been fixed in version 4.2.0-1+deb11u1. We recommend that you upgrade your tiff packages. For the detailed security status of tiff please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tiff

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/tiff
https://www.debian.org/security/2022/dsa-5108
https://security-tracker.debian.org/tracker/CVE-2022-0561
https://security-tracker.debian.org/tracker/CVE-2022-0562
https://security-tracker.debian.org/tracker/CVE-2022-0865
https://security-tracker.debian.org/tracker/CVE-2022-0891
https://security-tracker.debian.org/tracker/CVE-2022-0907
https://security-tracker.debian.org/tracker/CVE-2022-0908
https://security-tracker.debian.org/tracker/CVE-2022-0909
https://security-tracker.debian.org/tracker/CVE-2022-0924
https://security-tracker.debian.org/tracker/CVE-2022-22844
https://packages.debian.org/source/buster/tiff
https://packages.debian.org/source/bullseye/tiff

Solution

Upgrade the tiff packages.

For the stable distribution (bullseye), these problems have been fixed in version 4.2.0-1+deb11u1.

Risk Factor

Medium

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/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-2022-0561
CVE	CVE-2022-0562
CVE	CVE-2022-0865
CVE	CVE-2022-0891
CVE	CVE-2022-0907
CVE	CVE-2022-0908

CVE	CVE-2022-0909
CVE	CVE-2022-0924
CVE	CVE-2022-22844

Plugin Information

Published: 2022/03/25, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u4
```

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
```

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+deb10u2
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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u3
Remote package installed : libcurl4_7.64.0-4+deb10u2
Should be : libcurl4_7.64.0-4+deb10u3
```

164935 - Debian dla-3101 : libxslt1-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-3101 advisory.

- ---------- Debian LTS Advisory DLA-3101-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 09, 2022 https://wiki.debian.org/LTS
- ----------

Package : libxslt Version : 1.1.32-2.2~deb10u2 CVE ID : CVE-2019-5815 CVE-2021-30560

Two vulnerabilities were discovered in libxslt, an XSLT processing runtime library, that could result in denial of service or potentially the execution of arbitrary code if malicious files are processed.

For Debian 10 buster, these problems have been fixed in version 1.1.32-2.2~deb10u2.

We recommend that you upgrade your libxslt packages.

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

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/libxslt
https://security-tracker.debian.org/tracker/CVE-2019-5815
https://security-tracker.debian.org/tracker/CVE-2021-30560
https://packages.debian.org/source/buster/libxslt

Solution

Upgrade the libxslt1-dev 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

6.8 (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-2019-5815
CVE	CVE-2021-30560

Plugin Information

Published: 2022/09/10, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libxslt1.1_1.1.32-2.2~deb10u1
Should be : libxslt1.1_1.1.32-2.2~deb10u2
```

165206 - Debian dla-3110 : libglib2.0-0 - 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-3110 advisory.

- ---------- Debian LTS Advisory DLA-3110-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 15, 2022 https://wiki.debian.org/LTS
- ----------

Package : glib2.0 Version : 2.58.3-2+deb10u4 CVE ID : CVE-2021-3800

It was found that GLib, a general-purpose portable utility library, could be used to print partial contents from arbitrary files. This could be exploited from setuid binaries linking to GLib for information disclosure of files with a specific format.

For Debian 10 buster, this problem has been fixed in version 2.58.3-2+deb10u4.

We recommend that you upgrade your glib2.0 packages.

For the detailed security status of glib2.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glib2.0

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/glib2.0
https://security-tracker.debian.org/tracker/CVE-2021-3800
https://packages.debian.org/source/buster/glib2.0

Solution

Upgrade the libglib2.0-0 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:H/I:N/A:N)

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-3800

Plugin Information

Published: 2022/09/15, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.58.3-2+deb10u3
Should be : libglib2.0-0_2.58.3-2+deb10u4
Remote package installed : libglib2.0-data_2.58.3-2+deb10u3
Should be : libglib2.0-data_2.58.3-2+deb10u4
```

165219 - Debian dla-3114 : libmariadb-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-3114 advisory.

- ---------- Debian LTS Advisory DLA-3114-2 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 30, 2022 https://wiki.debian.org/LTS
- ----------

Package : mariadb-10.3 Version : 1:10.3.36-0+deb10u2 Debian Bug : 1020301

The update for mariadb-10.3 released as DLA-3114 introduced a bug in the mariadb-server-10.3 package, that could cause installation failures when installing or updating plugin packages.

For Debian 10 buster, this problem has been fixed in version 1:10.3.36-0+deb10u2.

We recommend that you upgrade your mariadb-10.3 packages.

For the detailed security status of mariadb-10.3 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/mariadb-10.3

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

http://www.nessus.org/u?cb6537b5
https://packages.debian.org/source/buster/mariadb-10.3

Solution

Upgrade the libmariadb-dev packages.

Risk Factor

Medium

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libmariadb3_1:10.3.29-0+deb10u1
Should be : libmariadb3_1:10.3.36-0+deb10u2
Remote package installed : mariadb-client_1:10.3.29-0+deb10u1
```

```
Should be : mariadb-client_1:10.3.36-0+deb10u2
Remote package installed : mariadb-client-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-10.3_1:10.3.36-0+deb10u2
Remote package installed : mariadb-client-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-core-10.3_1:10.3.36-0+deb10u2
Remote package installed : mariadb-common_1:10.3.29-0+deb10u1
Should be : mariadb-common_1:10.3.36-0+deb10u2
Remote package installed : mariadb-server_1:10.3.29-0+deb10u1
Should be : mariadb-server_1:10.3.36-0+deb10u2
Remote package installed : mariadb-server-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-10.3_1:10.3.36-0+deb10u2
Remote package installed : mariadb-server-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-core-10.3_1:10.3.36-0+deb10u2
```

165327 - Debian dla-3118 : unzip - 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-3118 advisory.

- ---------- Debian LTS Advisory DLA-3118-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort September 22, 2022 https://wiki.debian.org/LTS
- ----------

Package : unzip Version : 6.0-23+deb10u3 CVE ID : CVE-2022-0529 CVE-2022-0530 Debian Bug : 1010355

Sandipan Roy discovered two vulnerabilities in InfoZIP's unzip program, a de-archiver for .zip files, which could result in denial of service or potentially the execution of arbitrary code.

For Debian 10 buster, these problems have been fixed in version 6.0-23+deb10u3.

We recommend that you upgrade your unzip packages.

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

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/unzip
https://security-tracker.debian.org/tracker/CVE-2022-0529
https://security-tracker.debian.org/tracker/CVE-2022-0530
https://packages.debian.org/source/buster/unzip

Solution

Upgrade the unzip 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-2022-0529
CVE	CVE-2022-0530

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : unzip_6.0-23+deb10u2
Should be : unzip_6.0-23+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
```

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+deb10u1
Should be : isc-dhcp-client_4.4.1-2+deb10u2
Remote package installed : isc-dhcp-common_4.4.1-2+deb10u1
Should be : isc-dhcp-common_4.4.1-2+deb10u2
```

166429 - Debian dla-3157 : bluetooth - 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-3157 advisory.

- ---------- Debian LTS Advisory DLA-3157-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler October 24, 2022 https://wiki.debian.org/LTS
- ----------

Package : bluez Version : 5.50-1.2~deb10u3 CVE ID : CVE-2019-8921 CVE-2019-8922 CVE-2021-41229 CVE-2021-43400 CVE-2022-0204 CVE-2022-39176 CVE-2022-39177 Debian Bug : 998626 1000262 1003712

Several vulnerabilities were discovered in BlueZ, the Linux Bluetooth protocol stack. An attacker could cause a denial-of-service (DoS) or leak information.

CVE-2019-8921

SDP infoleak, the vulnerability lies in the handling of a SVC_ATTR_REQ by the SDP implementation of BlueZ. By crafting a malicious CSTATE, it is possible to trick the server into returning more bytes than the buffer actually holds, resulting in leaking arbitrary heap data.

CVE-2019-8922

SDP Heap Overflow; this vulnerability lies in the SDP protocol handling of attribute requests as well. By requesting a huge number of attributes at the same time, an attacker can overflow the static buffer provided to hold the response.

CVE-2021-41229

sdp_cstate_alloc_buf allocates memory which will always be hung in the singly linked list of cstates and will not be freed. This will cause a memory leak over time. The data can be a very large object, which can be caused by an attacker continuously sending sdp packets and this may cause the service of the target device to crash.

CVE-2021-43400

A use-after-free in gatt-database.c can occur when a client disconnects during D-Bus processing of a WriteValue call.

CVE-2022-0204

A heap overflow vulnerability was found in bluez. An attacker with local network access could pass specially crafted files causing an application to halt or crash, leading to a denial of service.

CVE-2022-39176

BlueZ allows physically proximate attackers to obtain sensitive information because profiles/audio/avrcp.c does not validate params_len.

CVE-2022-39177

BlueZ allows physically proximate attackers to cause a denial of service because malformed and invalid capabilities can be processed in profiles/audio/avdtp.c.

For Debian 10 buster, these problems have been fixed in version 5.50-1.2~deb10u3.

We recommend that you upgrade your bluez packages.

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

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/bluez
https://security-tracker.debian.org/tracker/CVE-2019-8921
https://security-tracker.debian.org/tracker/CVE-2019-8922
https://security-tracker.debian.org/tracker/CVE-2021-41229
https://security-tracker.debian.org/tracker/CVE-2021-43400
https://security-tracker.debian.org/tracker/CVE-2022-0204
https://security-tracker.debian.org/tracker/CVE-2022-39176
https://security-tracker.debian.org/tracker/CVE-2022-39177
https://packages.debian.org/source/buster/bluez

Solution

Upgrade the bluetooth 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:H/A:N)

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:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-8921
CVE	CVE-2019-8922
CVE	CVE-2021-41229
CVE	CVE-2021-43400
CVE	CVE-2022-0204
CVE	CVE-2022-39176
CVE	CVE-2022-39177

Plugin Information

Published: 2022/10/24, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : bluetooth_5.50-1.2~deb10u1
Should be : bluetooth_5.50-1.2~deb10u3
Remote package installed : bluez_5.50-1.2~deb10u1
Should be : bluez_5.50-1.2~deb10u3
```

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
```

167912 - Debian dla-3198 : php-phpseclib - 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-3198 advisory.

- ---------- Debian LTS Advisory DLA-3198-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler November 17, 2022 https://wiki.debian.org/LTS
- ----------

Package : php-phpseclib Version : 2.0.30-2~deb10u1 CVE ID : CVE-2021-30130

It was discovered that php-phpseclib, a pure-PHP implementation of various cryptographic and arithmetic algorithms (v2), mishandles RSA PKCS#1 v1.5 signature verification. An attacker may get invalid signatures accepted, bypassing authorization control in specific situations.

For Debian 10 buster, this problem has been fixed in version 2.0.30-2~deb10u1.

We recommend that you upgrade your php-phpseclib packages.

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

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

http://www.nessus.org/u?bb7f1a05
https://security-tracker.debian.org/tracker/CVE-2021-30130
https://packages.debian.org/source/buster/php-phpseclib

Solution

Upgrade the php-phpseclib 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:N/I:H/A:N)

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:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-30130

Plugin Information

Published: 2022/11/18, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : php-phpseclib_2.0.14-1
Should be : php-phpseclib_2.0.30-2~deb10u1
```

168859 - Debian dla-3243 : libapache2-mod-php7.3 - 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-3243 advisory.

- ---------- Debian LTS Advisory DLA-3243-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort December 15, 2022 https://wiki.debian.org/LTS
- ----------

Package : php7.3 Version : 7.3.31-1~deb10u2 CVE ID : CVE-2021-21707 CVE-2022-31625 CVE-2022-31626 CVE-2022-31628 CVE-2022-31629 CVE-2022-37454

Multiple security issues were discovered in PHP, a widely-used open source general purpose scripting language which could result in denial of service, information disclosure, insecure cooking handling or potentially the execution of arbitrary code.

For Debian 10 buster, these problems have been fixed in version 7.3.31-1~deb10u2.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2021-21707
https://security-tracker.debian.org/tracker/CVE-2022-31625
https://security-tracker.debian.org/tracker/CVE-2022-31626
https://security-tracker.debian.org/tracker/CVE-2022-31628
https://security-tracker.debian.org/tracker/CVE-2022-31629
https://security-tracker.debian.org/tracker/CVE-2022-37454

https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 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

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-2021-21707
CVE	CVE-2022-31625
CVE	CVE-2022-31626
CVE	CVE-2022-31628
CVE	CVE-2022-31629
CVE	CVE-2022-37454
XREF	IAVA:2022-A-0515-S

Plugin Information

Published: 2022/12/16, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
Should be : libapache2-mod-php7.3_7.3.31-1~deb10u2
Remote package installed : php7.3_7.3.29-1~deb10u1
Should be : php7.3_7.3.31-1~deb10u2
Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
Should be : php7.3-cgi_7.3.31-1~deb10u2
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u2
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u2
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u2
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u2
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u2
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u2
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u2
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u2
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u2
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u2
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u2
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u2
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u2
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u2
```

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
```

170240 - Debian dla-3278 : libtiff-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-3278 advisory.

- ---------- Debian LTS Advisory DLA-3278-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sylvain Beucler January 20, 2023 https://wiki.debian.org/LTS
- ----------

Package : tiff Version : 4.1.0+git191117-2~deb10u5 CVE ID : CVE-2022-1354 CVE-2022-1355 CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-3570 CVE-2022-3597 CVE-2022-3598 CVE-2022-3599 CVE-2022-3626 CVE-2022-3627 CVE-2022-3970 CVE-2022-34526 Debian Bug : 1011160 1014494 1022555 1024737

Multiple vulnerabilities were found in tiff, a library and tools providing support for the Tag Image File Format (TIFF), leading to denial of service (DoS) and possibly local code execution.

CVE-2022-1354

A heap buffer overflow flaw was found in Libtiffs' tiffinfo.c in TIFFReadRawDataStriped() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffinfo tool, triggering a heap buffer overflow issue and causing a crash that leads to a denial of service.

CVE-2022-1355

A stack buffer overflow flaw was found in Libtiffs' tiffcp.c in main() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffcp tool, triggering a stack buffer overflow issue, possibly corrupting the memory, and causing a crash that leads to a denial of service.

CVE-2022-2056, CVE-2022-2057, CVE-2022-2058

Divide By Zero error in tiffcrop allows attackers to cause a denial-of-service via a crafted tiff file.

CVE-2022-2867, CVE-2022-2868, CVE-2022-2869

libtiff's tiffcrop utility has underflow and input validation flaw that can lead to out of bounds read and write. An attacker who supplies a crafted file to tiffcrop (likely via tricking a user to run tiffcrop on it with certain parameters) could cause a crash or in some cases, further exploitation.

CVE-2022-3570, CVE-2022-3598

Multiple heap buffer overflows in tiffcrop.c utility in libtiff allows attacker to trigger unsafe or out of bounds memory access via crafted TIFF image file which could result into application crash, potential information disclosure or any other context-dependent impact.

CVE-2022-3597, CVE-2022-3626, CVE-2022-3627

Out-of-bounds write, allowing attackers to cause a denial-of-service via a crafted tiff file.

CVE-2022-3599

Out-of-bounds read in writeSingleSection in tools/tiffcrop.c, allowing attackers to cause a denial-of-service via a crafted tiff file.

CVE-2022-3970

Affects the function TIFFReadRGBATileExt of the file libtiff/tif_getimage.c. The manipulation leads to integer overflow.

CVE-2022-34526

A stack overflow was discovered in the _TIFFVGetField function of Tiffsplit. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted TIFF file parsed by the tiffsplit or tiffcrop utilities.

For Debian 10 buster, these problems have been fixed in version 4.1.0+git191117-2~deb10u5.

We recommend that you upgrade your tiff packages.

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

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/tiff
https://security-tracker.debian.org/tracker/CVE-2022-1354
https://security-tracker.debian.org/tracker/CVE-2022-1355
https://security-tracker.debian.org/tracker/CVE-2022-2056
https://security-tracker.debian.org/tracker/CVE-2022-2057
https://security-tracker.debian.org/tracker/CVE-2022-2058
https://security-tracker.debian.org/tracker/CVE-2022-2867
https://security-tracker.debian.org/tracker/CVE-2022-2868
https://security-tracker.debian.org/tracker/CVE-2022-2869
https://security-tracker.debian.org/tracker/CVE-2022-34526
https://security-tracker.debian.org/tracker/CVE-2022-3570
https://security-tracker.debian.org/tracker/CVE-2022-3597
https://security-tracker.debian.org/tracker/CVE-2022-3598
https://security-tracker.debian.org/tracker/CVE-2022-3599
https://security-tracker.debian.org/tracker/CVE-2022-3626
https://security-tracker.debian.org/tracker/CVE-2022-3627
https://security-tracker.debian.org/tracker/CVE-2022-3970
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the libtiff-dev 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

7.9 (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-2022-1354
CVE	CVE-2022-1355
CVE	CVE-2022-2056
CVE	CVE-2022-2057
CVE	CVE-2022-2058
CVE	CVE-2022-2867
CVE	CVE-2022-2868
CVE	CVE-2022-2869
CVE	CVE-2022-3570
CVE	CVE-2022-3597
CVE	CVE-2022-3598
CVE	CVE-2022-3599
CVE	CVE-2022-3626
CVE	CVE-2022-3627
CVE	CVE-2022-3970
CVE	CVE-2022-34526

Plugin Information

Published: 2023/01/21, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u4
Remote package installed : libcurl4_7.64.0-4+deb10u2
Should be : libcurl4_7.64.0-4+deb10u4
```

170881 - Debian dla-3297 : libtiff-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-3297 advisory.

- ---------- Debian LTS Advisory DLA-3297-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Utkarsh Gupta January 31, 2023 https://wiki.debian.org/LTS
- ----------

Package : tiff Version : 4.1.0+git191117-2~deb10u6 CVE ID : CVE-2022-48281 Debian Bug : 1029653

processCropSelections in tools/tiffcrop.c in LibTIFF, the Tag Image File Format (TIFF) library and tools, has a heap-based buffer overflow (e.g., WRITE of size 307203) via a crafted TIFF image.

For Debian 10 buster, this problem has been fixed in version 4.1.0+git191117-2~deb10u6.

We recommend that you upgrade your tiff packages.

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

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/tiff
https://security-tracker.debian.org/tracker/CVE-2022-48281
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the libtiff-dev 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

4.9 (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)

References

CVE CVE-2022-48281

Plugin Information

Published: 2023/01/31, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u6
```

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+deb10u6
Should be : libssl1.1_1.1.1n-0+deb10u4
Remote package installed : openssl_1.1.1d-0+deb10u6
Should be : openssl_1.1.1n-0+deb10u4
```

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
```

171785 - Debian dla-3333 : libtiff-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-3333 advisory.

---------- Debian LTS Advisory DLA-3333-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany February 21, 2023 https://wiki.debian.org/LTS

Package : tiff Version : 4.1.0+git191117-2~deb10u7 CVE ID : CVE-2023-0795 CVE-2023-0796 CVE-2023-0797 CVE-2023-0798 CVE-2023-0799 CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804 Debian Bug : 1031632

Several flaws were found in tiffcrop, a program distributed by tiff, a library and tools providing support for the Tag Image File Format (TIFF).
A specially crafted tiff file can lead to an out-of-bounds write or read resulting in a denial of service.

For Debian 10 buster, these problems have been fixed in version 4.1.0+git191117-2~deb10u7.

We recommend that you upgrade your tiff packages.

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

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/tiff
https://security-tracker.debian.org/tracker/CVE-2023-0795
https://security-tracker.debian.org/tracker/CVE-2023-0796
https://security-tracker.debian.org/tracker/CVE-2023-0797
https://security-tracker.debian.org/tracker/CVE-2023-0798
https://security-tracker.debian.org/tracker/CVE-2023-0799
https://security-tracker.debian.org/tracker/CVE-2023-0800
https://security-tracker.debian.org/tracker/CVE-2023-0801
https://security-tracker.debian.org/tracker/CVE-2023-0802
https://security-tracker.debian.org/tracker/CVE-2023-0803
https://security-tracker.debian.org/tracker/CVE-2023-0804
https://packages.debian.org/source/buster/tiff

Solution

Upgrade the libtiff-dev 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

4.9 (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)

References

CVE	CVE-2023-0795
CVE	CVE-2023-0796
CVE	CVE-2023-0797
CVE	CVE-2023-0798
CVE	CVE-2023-0799
CVE	CVE-2023-0800
CVE	CVE-2023-0801
CVE	CVE-2023-0802
CVE	CVE-2023-0803
CVE	CVE-2023-0804

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.1.0+git191117-2~deb10u2
Should be : libtiff5_4.1.0+git191117-2~deb10u7
```

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+deb10u5
Should be : apache2_2.4.38-3+deb10u9
Remote package installed : apache2-bin_2.4.38-3+deb10u5
Should be : apache2-bin_2.4.38-3+deb10u9
Remote package installed : apache2-data_2.4.38-3+deb10u5
Should be : apache2-data_2.4.38-3+deb10u9
Remote package installed : apache2-doc_2.4.38-3+deb10u5
Should be : apache2-doc_2.4.38-3+deb10u9
Remote package installed : apache2-utils_2.4.38-3+deb10u5
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
```

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 : libnss-systemd_241-7~deb10u7
Should be : libnss-systemd_241-7~deb10u9
Remote package installed : libpam-systemd_241-7~deb10u7
Should be : libpam-systemd_241-7~deb10u9
Remote package installed : libsystemd0_241-7~deb10u7
Should be : libsystemd0_241-7~deb10u9
Remote package installed : libudev1_241-7~deb10u7
Should be : libudev1_241-7~deb10u9
Remote package installed : systemd_241-7~deb10u7
Should be : systemd_241-7~deb10u9
Remote package installed : systemd-sysv_241-7~deb10u7
Should be : systemd-sysv_241-7~deb10u9
Remote package installed : udev_241-7~deb10u7
Should be : udev_241-7~deb10u9
```

175045 - Debian dla-3414 : avahi-autoipd - 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-3414 advisory.

- ---------- Debian LTS Advisory DLA-3414-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb May 02, 2023 https://wiki.debian.org/LTS
- ----------

Package : avahi Version : 0.7-4+deb10u2 CVE ID : CVE-2023-1981 Debian Bug : 1034594

It was discovered that there was a local Denial of Service (DoS) vulnerability in Avahi, a system that facilitates service discovery on a local network.

The avahi-daemon process could have been crashed over the DBus message bus.

For Debian 10 buster, this problem has been fixed in version 0.7-4+deb10u2.

We recommend that you upgrade your avahi packages.

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

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-2023-1981
https://security-tracker.debian.org/tracker/source-package/avahi
https://packages.debian.org/source/buster/avahi

Solution

Upgrade the avahi-autoipd 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-2023-1981

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : avahi-autoipd_0.7-4+deb10u1
Should be : avahi-autoipd_0.7-4+deb10u2
```

176730 - Debian dla-3444 : libmariadb-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-3444 advisory.

- ---------- Debian LTS Advisory DLA-3444-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Otto Keklinen June 03, 2023 https://wiki.debian.org/LTS
- ----------

Package : mariadb-10.3 Version : 1:10.3.39-0+deb10u1 CVE ID : CVE-2022-47015 Debian Bug : 1034889

Latest MariaDB minor maintenance release 10.3.39 included a fix for the following security vulnerability:

CVE-2022-47015

Spider storage engine vulnerable to Denial of Service

For Debian 10 buster, this problem has been fixed in version 1:10.3.39-0+deb10u1.

Additionally the backwards incompatible libmariadb API change has been reverted (Closes: #1031773).

We recommend that you upgrade your mariadb-10.3 packages.

For the detailed security status of mariadb-10.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.3

Note! According to https://mariadb.org/about/#maintenance-policy this was the last minor maintenance release for MariaDB 10.3 series.

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-2022-47015
https://packages.debian.org/source/buster/mariadb-10.3
http://www.nessus.org/u?cb6537b5

Solution

Upgrade the libmariadb-dev 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

5.7 (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-2022-47015

Plugin Information

Published: 2023/06/06, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libmariadb3_1:10.3.29-0+deb10u1
Should be : libmariadb3_1:10.3.39-0+deb10u1
Remote package installed : mariadb-client_1:10.3.29-0+deb10u1
Should be : mariadb-client_1:10.3.39-0+deb10u1
Remote package installed : mariadb-client-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-10.3_1:10.3.39-0+deb10u1
Remote package installed : mariadb-client-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-core-10.3_1:10.3.39-0+deb10u1
Remote package installed : mariadb-common_1:10.3.29-0+deb10u1
Should be : mariadb-common_1:10.3.39-0+deb10u1
Remote package installed : mariadb-server_1:10.3.29-0+deb10u1
Should be : mariadb-server_1:10.3.39-0+deb10u1
Remote package installed : mariadb-server-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-10.3_1:10.3.39-0+deb10u1
Remote package installed : mariadb-server-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-core-10.3_1:10.3.39-0+deb10u1
```

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+deb10u6
Should be : libssl1.1_1.1.1n-0+deb10u5
Remote package installed : openssl_1.1.1d-0+deb10u6
Should be : openssl_1.1.1n-0+deb10u5
```

177421 - Debian dla-3456 : python-requests - 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-3456 advisory.

---------- Debian LTS Advisory DLA-3456-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany June 18, 2023 https://wiki.debian.org/LTS

Package : requests Version : 2.21.0-1+deb10u1 CVE ID : CVE-2023-32681 Debian Bug : 1036693

Requests, a Python HTTP library, has been leaking Proxy-Authorization headers to destination servers when redirected to an HTTPS endpoint. For HTTP connections sent through the tunnel, the proxy will identify the header in the request itself and remove it prior to forwarding to the destination server. However when sent over HTTPS, the `Proxy-Authorization` header must be sent in the CONNECT request as the proxy has no visibility into the tunneled request. This results in Requests forwarding proxy credentials to the destination server unintentionally, allowing a malicious actor to potentially exfiltrate sensitive information.

For Debian 10 buster, this problem has been fixed in version 2.21.0-1+deb10u1.

We recommend that you upgrade your requests packages.

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

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/requests
https://security-tracker.debian.org/tracker/CVE-2023-32681
https://packages.debian.org/source/buster/requests

Solution

Upgrade the python-requests 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

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

CVSS v3.0 Temporal Score

5.5 (CVSS:3.0/E:P/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

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

References

CVE CVE-2023-32681

Plugin Information

Published: 2023/06/18, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : python3-requests_2.21.0-1
Should be : python3-requests_2.21.0-1+deb10u1
```

177451 - Debian dla-3458 : libapache2-mod-php7.3 - 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-3458 advisory.

---------- Debian LTS Advisory DLA-3458-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin June 20, 2023 https://wiki.debian.org/LTS

Package : php7.3 Version : 7.3.31-1~deb10u4 CVE ID : CVE-2023-3247

Niels Dossche and Tim Dsterhus discovered that PHP's implementation of the SOAP HTTP Digest authentication did not check for failures, which may result in a stack information leak. Furthermore, the code used an insufficient number of random bytes.

For Debian 10 buster, this problem has been fixed in version 7.3.31-1~deb10u4.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2023-3247
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3247
XREF	IAVA:2023-A-0321-S

Plugin Information

Published: 2023/06/20, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
Should be : libapache2-mod-php7.3_7.3.31-1~deb10u4
Remote package installed : php7.3_7.3.29-1~deb10u1
Should be : php7.3_7.3.31-1~deb10u4
Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
Should be : php7.3-cgi_7.3.31-1~deb10u4
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u4
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u4
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u4
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u4
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u4
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u4
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u4
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u4
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u4
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u4
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u4
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u4
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u4
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u4
```

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 : libnss-systemd_241-7~deb10u7
Should be : libnss-systemd_241-7~deb10u10
Remote package installed : libpam-systemd_241-7~deb10u7
Should be : libpam-systemd_241-7~deb10u10
Remote package installed : libsystemd0_241-7~deb10u7
Should be : libsystemd0_241-7~deb10u10
Remote package installed : libudev1_241-7~deb10u7
Should be : libudev1_241-7~deb10u10
Remote package installed : systemd_241-7~deb10u7
Should be : systemd_241-7~deb10u10
Remote package installed : systemd-sysv_241-7~deb10u7
Should be : systemd-sysv_241-7~deb10u10
Remote package installed : udev_241-7~deb10u7
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+deb10u6
Should be : libssl1.1_1.1.1n-0+deb10u6
Remote package installed : openssl_1.1.1d-0+deb10u6
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 : libdw1_0.176-1.1
Should be : libdw1_0.176-1.1+deb10u1
```

```
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+deb10u2
Should be : libx11-6_2:1.6.7-1+deb10u4
Remote package installed : libx11-data_2:1.6.7-1+deb10u2
Should be : libx11-data_2:1.6.7-1+deb10u4
```

182585 - Debian dla-3603 : libxpm-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-3603 advisory.

- ---------- Debian LTS Advisory DLA-3603-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Emilio Pozuelo Monfort October 05, 2023 https://wiki.debian.org/LTS
- ----------

Package : libxpm Version : 1:3.5.12-1+deb10u2 CVE ID : CVE-2023-43786 CVE-2023-43787 CVE-2023-43788 CVE-2023-43789

Several vulnerabilities were found in libXpm, the X Pixmap (XPM) image library.

CVE-2023-43786

Yair Mizrahi discovered an infinite recursion issue when parsing crafted XPM files, which would result in denial of service.

CVE-2023-43787

Yair Mizrahi discovered a buffer overflow vulnerability in libX11 when parsing crafted XPM files, which could result in denial of service or potentially the execution of arbitrary code.

CVE-2023-43788

Alan Coopersmith found an out of bounds read in XpmCreateXpmImageFromBuffer, which could result in denial of service when parsing crafted XPM files.

CVE-2023-43789

Alan Coopersmith discovered an out of bounds read issue when parsing corrupted colormaps, which could lead to denial of service when parsing crafted XPM files.

For Debian 10 buster, these problems have been fixed in version 1:3.5.12-1+deb10u2.

We recommend that you upgrade your libxpm packages.

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

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/libxpm
https://security-tracker.debian.org/tracker/CVE-2023-43786
https://security-tracker.debian.org/tracker/CVE-2023-43787
https://security-tracker.debian.org/tracker/CVE-2023-43788
https://security-tracker.debian.org/tracker/CVE-2023-43789
https://packages.debian.org/source/buster/libxpm

Solution

Upgrade the libxpm-dev 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-2023-43786
CVE	CVE-2023-43787
CVE	CVE-2023-43788
CVE	CVE-2023-43789

Plugin Information

Published: 2023/10/05, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libxpm4_1:3.5.12-1
Should be : libxpm4_1:3.5.12-1+deb10u2
```

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
```

182762 - Debian dla-3610 : python-urllib3 - 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-3610 advisory.

---------- Debian LTS Advisory DLA-3610-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin October 08, 2023 https://wiki.debian.org/LTS

Package : python-urllib3 Version : 1.24.1-1+deb10u1 CVE ID : CVE-2019-11236 CVE-2019-11324 CVE-2020-26137 CVE-2023-43804 Debian Bug : 927172 927412 1053626

Security vulnerabilities were found in python-urllib3, an HTTP library with thread-safe connection pooling for Python, which could lead to information disclosure or authorization bypass.

CVE-2019-11236

Hanno Bck discovered that an attacker controlling the request parameter can inject headers by injecting CR/LF chars. The issue is similar to CPython's CVE-2019-9740.

CVE-2019-11324

Christian Heimes discovered that when verifying HTTPS connections upon passing an SSLContext to urllib3, system CA certificates are loaded into the SSLContext by default in addition to any manually-specified CA certificates.
This causes TLS handshakes that should fail given only the manually specified certs to succeed based on system CA certs.

CVE-2020-26137

It was discovered that CRLF injection was possible if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest().
The issue is similar to urllib's CVE-2020-26116.

CVE-2023-43804

It was discovered that the Cookie request header isn't stripped during cross-origin redirects. It is therefore possible for a user specifying a Cookie header to unknowingly leak information via HTTP redirects to a different origin (unless the user disables redirects explicitly). The issue is similar to CVE-2018-20060, but for Cookie request header rather than Authorization.

Moreover authorization request headers were not removed redirecting to cross-site. Per RFC7230 sec. 3.2 header fields are to be treated case-insensitively.

For Debian 10 buster, these problems have been fixed in version 1.24.1-1+deb10u1.

We recommend that you upgrade your python-urllib3 packages.

For the detailed security status of python-urllib3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python-urllib3

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

http://www.nessus.org/u?eb907009
https://packages.debian.org/source/buster/python-urllib3
https://security-tracker.debian.org/tracker/CVE-2018-20060
https://security-tracker.debian.org/tracker/CVE-2019-9740
https://security-tracker.debian.org/tracker/CVE-2019-11236
https://security-tracker.debian.org/tracker/CVE-2019-11324
https://security-tracker.debian.org/tracker/CVE-2020-26116
https://security-tracker.debian.org/tracker/CVE-2020-26137
https://security-tracker.debian.org/tracker/CVE-2023-43804

Solution

Upgrade the python-urllib3 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

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)

References

CVE	CVE-2018-20060
CVE	CVE-2019-9740
CVE	CVE-2019-11236
CVE	CVE-2019-11324
CVE	CVE-2020-26116
CVE	CVE-2020-26137
CVE	CVE-2023-43804

Plugin Information

Published: 2023/10/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : python3-urllib3_1.24.1-1
Should be : python3-urllib3_1.24.1-1+deb10u1
```

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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u7
Remote package installed : libcurl4_7.64.0-4+deb10u2
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
```

185377 - Debian dla-3649 : python-urllib3 - 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-3649 advisory.

---------- Debian LTS Advisory DLA-3649-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Sean Whitton November 08, 2023 https://wiki.debian.org/LTS

Package : python-urllib3 Version : 1.24.1-1+deb10u2 CVE ID : CVE-2023-43803 Debian Bug : 1054226

It was discovered that python-urllib3, a user-friendly HTTP client library for Python, did not remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could accept a request body, like POST, to GET, as required by the HTTP RFCs. This could lead to information disclosure.

For Debian 10 buster, these problems have been fixed in version 1.24.1-1+deb10u2.

We recommend that you upgrade your python-urllib3 packages.

For the detailed security status of python-urllib3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python-urllib3

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?eb907009
https://security-tracker.debian.org/tracker/CVE-2023-43803
https://packages.debian.org/source/buster/python-urllib3

Solution

Upgrade the python-urllib3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-43803

Plugin Information

Published: 2023/11/08, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : python3-urllib3_1.24.1-1
Should be : python3-urllib3_1.24.1-1+deb10u2
```

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+deb10u7
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
```

186966 - Debian dla-3689 : bluetooth - 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-3689 advisory.

- ---------- Debian LTS Advisory DLA-3689-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Chris Lamb December 14, 2023 https://wiki.debian.org/LTS
- ----------

Package : bluez Version : 5.50-1.2~deb10u4 CVE ID : CVE-2023-45866 Debian Bug : 1057914

It was discovered that there was a keyboard injection attack in Bluez, a set of services and tools for interacting with wireless Bluetooth devices.

Prior to this change, BlueZ may have permitted an unauthenticated peripherals to establish encrypted connections and thereby accept keyboard reports, potentially permitting injection of HID (~keyboard) commands, despite no user authorising such access.

For Debian 10 buster, this problem has been fixed in version 5.50-1.2~deb10u4.

We recommend that you upgrade your bluez packages.

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

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://packages.debian.org/source/buster/bluez
https://security-tracker.debian.org/tracker/CVE-2023-45866
https://security-tracker.debian.org/tracker/source-package/bluez

Solution

Upgrade the bluetooth packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-45866

Plugin Information

Published: 2023/12/15, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : bluetooth_5.50-1.2~deb10u1
Should be : bluetooth_5.50-1.2~deb10u4
Remote package installed : bluez_5.50-1.2~deb10u1
Should be : bluez_5.50-1.2~deb10u4
```

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+deb10u2
Should be : libcurl3-gnutls_7.64.0-4+deb10u8
Remote package installed : libcurl4_7.64.0-4+deb10u2
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
```

189489 - Debian dla-3718 : php-phpseclib - 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-3718 advisory.

---------- Debian LTS Advisory DLA-3718-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Guilhem Moulin January 25, 2024 https://wiki.debian.org/LTS

Package : php-phpseclib Version : 2.0.30-2~deb10u2 CVE ID : CVE-2023-48795

It was discovered that php-phpseclib, a PHP library for arbitrary-precision integer arithmetic, was vulnerable to the so-called Terrapin Attack.

The SSH transport protocol with certain OpenSSH extensions, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC).

For Debian 10 buster, this problem has been fixed in version 2.0.30-2~deb10u2.

We recommend that you upgrade your php-phpseclib packages.

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

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?bb7f1a05
https://security-tracker.debian.org/tracker/CVE-2023-48795
https://packages.debian.org/source/buster/php-phpseclib

Solution

Upgrade the php-phpseclib 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: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: 2024/01/25, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : php-phpseclib_2.0.14-1
Should be : php-phpseclib_2.0.30-2~deb10u2
```

189721 - Debian dla-3722 : libmariadb-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-3722 advisory.

- ---------- Debian LTS Advisory DLA-3722-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien ROUCARI?S January 27, 2024 https://wiki.debian.org/LTS
- ----------

Package : mariadb-10.3 Version : 1:10.3.39-0+deb10u2 CVE ID : CVE-2023-22084 Debian Bug : 1055034

A vulnerability was fixed in MariaDB, a database suite.
This vulnerability allowed a high privileged attacker with network access to compromise a MariaDB Server.
Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash.

The main risk was a complete DOS of the sever.

For Debian 10 buster, this problem has been fixed in version 1:10.3.39-0+deb10u2.

We recommend that you upgrade your mariadb-10.3 packages.

For the detailed security status of mariadb-10.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.3

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

http://www.nessus.org/u?cb6537b5
https://security-tracker.debian.org/tracker/CVE-2023-22084
https://packages.debian.org/source/buster/mariadb-10.3

Solution

Upgrade the libmariadb-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-22084

Plugin Information

Published: 2024/01/27, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libmariadb3_1:10.3.29-0+deb10u1
Should be : libmariadb3_1:10.3.39-0+deb10u2
Remote package installed : mariadb-client_1:10.3.29-0+deb10u1
Should be : mariadb-client_1:10.3.39-0+deb10u2
Remote package installed : mariadb-client-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-10.3_1:10.3.39-0+deb10u2
Remote package installed : mariadb-client-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-client-core-10.3_1:10.3.39-0+deb10u2
Remote package installed : mariadb-common_1:10.3.29-0+deb10u1
Should be : mariadb-common_1:10.3.39-0+deb10u2
Remote package installed : mariadb-server_1:10.3.29-0+deb10u1
Should be : mariadb-server_1:10.3.39-0+deb10u2
Remote package installed : mariadb-server-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-10.3_1:10.3.39-0+deb10u2
Remote package installed : mariadb-server-core-10.3_1:10.3.29-0+deb10u1
Should be : mariadb-server-core-10.3_1:10.3.39-0+deb10u2
```

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
```

193481 - Debian dla-3781 : libgd-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-3781 advisory.

- ---------- Debian LTS Advisory DLA-3781-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Thorsten Alteholz April 07, 2024 https://wiki.debian.org/LTS
- ----------

Package : libgd2 Version : 2.2.5-5.2+deb10u1 CVE ID : CVE-2018-14553 CVE-2021-38115 CVE-2021-40812

Several issues have been found in libgd2, a GD Graphics Library.
They are related to out-of-bounds reads or NULL pointer derefence allowing denial of service attacks.

For Debian 10 buster, these problems have been fixed in version 2.2.5-5.2+deb10u1.

We recommend that you upgrade your libgd2 packages.

For the detailed security status of libgd2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libgd2

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/libgd2
https://security-tracker.debian.org/tracker/CVE-2018-14553
https://security-tracker.debian.org/tracker/CVE-2021-38115
https://security-tracker.debian.org/tracker/CVE-2021-40812
https://packages.debian.org/source/buster/libgd2

Solution

Upgrade the libgd-dev 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: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

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-2018-14553
CVE	CVE-2021-38115
CVE	CVE-2021-40812

Plugin Information

Published: 2024/04/18, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : libgd3_2.2.5-5.2
Should be : libgd3_2.2.5-5.2+deb10u1
```

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+deb10u5
Should be : apache2_2.4.59-1~deb10u1
Remote package installed : apache2-bin_2.4.38-3+deb10u5
Should be : apache2-bin_2.4.59-1~deb10u1
Remote package installed : apache2-data_2.4.38-3+deb10u5
Should be : apache2-data_2.4.59-1~deb10u1
Remote package installed : apache2-doc_2.4.38-3+deb10u5
Should be : apache2-doc_2.4.59-1~deb10u1
Remote package installed : apache2-utils_2.4.38-3+deb10u5
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
```

200704 - Debian dla-3833 : libapache2-mod-php7.3 - 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-3833 advisory.

---------- Debian LTS Advisory DLA-3833-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany June 17, 2024 https://wiki.debian.org/LTS

Package : php7.3 Version : 7.3.31-1~deb10u7 CVE ID : CVE-2024-5458 Debian Bug : 1072885

PHP, a widely-used open source general purpose scripting language, is affected by a security problem when parsing certain types of URLs.

Due to a code logic error filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) will result in invalid user information (username + password part of URLs) being treated as valid user information.
This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. The problem is related to CVE-2020-7071 but affects IPv6 host parts.

For Debian 10 buster, this problem has been fixed in version 7.3.31-1~deb10u7.

We recommend that you upgrade your php7.3 packages.

For the detailed security status of php7.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.3

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/php7.3
https://security-tracker.debian.org/tracker/CVE-2020-7071
https://security-tracker.debian.org/tracker/CVE-2024-5458
https://packages.debian.org/source/buster/php7.3

Solution

Upgrade the libapache2-mod-php7.3 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

4.8 (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-2020-7071
CVE	CVE-2024-5458

Plugin Information

Published: 2024/06/18, Modified: 2024/06/18

Plugin Output

tcp/0

```
  Remote package installed : libapache2-mod-php7.3_7.3.29-1~deb10u1
  Should be : libapache2-mod-php7.3_7.3.31-1~deb10u7
  Remote package installed : php7.3_7.3.29-1~deb10u1
  Should be : php7.3_7.3.31-1~deb10u7
  Remote package installed : php7.3-cgi_7.3.29-1~deb10u1
```

```
Should be : php7.3-cgi_7.3.31-1~deb10u7
Remote package installed : php7.3-cli_7.3.29-1~deb10u1
Should be : php7.3-cli_7.3.31-1~deb10u7
Remote package installed : php7.3-common_7.3.29-1~deb10u1
Should be : php7.3-common_7.3.31-1~deb10u7
Remote package installed : php7.3-curl_7.3.29-1~deb10u1
Should be : php7.3-curl_7.3.31-1~deb10u7
Remote package installed : php7.3-gd_7.3.29-1~deb10u1
Should be : php7.3-gd_7.3.31-1~deb10u7
Remote package installed : php7.3-intl_7.3.29-1~deb10u1
Should be : php7.3-intl_7.3.31-1~deb10u7
Remote package installed : php7.3-json_7.3.29-1~deb10u1
Should be : php7.3-json_7.3.31-1~deb10u7
Remote package installed : php7.3-mbstring_7.3.29-1~deb10u1
Should be : php7.3-mbstring_7.3.31-1~deb10u7
Remote package installed : php7.3-mysql_7.3.29-1~deb10u1
Should be : php7.3-mysql_7.3.31-1~deb10u7
Remote package installed : php7.3-opcache_7.3.29-1~deb10u1
Should be : php7.3-opcache_7.3.31-1~deb10u7
Remote package installed : php7.3-readline_7.3.29-1~deb10u1
Should be : php7.3-readline_7.3.31-1~deb10u7
Remote package installed : php7.3-soap_7.3.29-1~deb10u1
Should be : php7.3-soap_7.3.31-1~deb10u7
Remote package installed : php7.3-xml_7.3.29-1~deb10u1
Should be : php7.3-xml_7.3.31-1~deb10u7
Remote package installed : php7.3-xmlrpc_7.3.29-1~deb10u1
Should be : php7.3-xmlrpc_7.3.31-1~deb10u7
Remote package installed : php7.3-zip_7.3.29-1~deb10u1
Should be : php7.3-zip_7.3.31-1~deb10u7
```

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
```

177492 - Debian dla-3466 : avahi-autoipd - 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-3466 advisory.

- ---------- Debian LTS Advisory DLA-3466-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Bastien Roucaris June 21, 2023 https://wiki.debian.org/LTS
- ----------

Package : avahi Version : 0.7-4+deb10u3 CVE ID : CVE-2021-3468 Debian Bug : 984938

Avahi a free zero-configuration networking (zeroconf) implementation, including a system for multicast DNS/DNS-SD service discovery, was affected by a Deny of Service. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop.

For Debian 10 buster, this problem has been fixed in version 0.7-4+deb10u3.

We recommend that you upgrade your avahi packages.

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

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/avahi
https://security-tracker.debian.org/tracker/CVE-2021-3468
https://packages.debian.org/source/buster/avahi

Solution

Upgrade the avahi-autoipd packages.

Risk Factor

Low

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-3468

Plugin Information

Published: 2023/06/22, Modified: 2025/01/22

Plugin Output

tcp/0

```
Remote package installed : avahi-autoipd_0.7-4+deb10u1
Should be : avahi-autoipd_0.7-4+deb10u3
```

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
Remote package installed : util-linux-locales_2.33.1-0.1
Should be : util-linux-locales_2.33.1-0.1+deb10u1
```

196946 - Debian dla-3814 : libglib2.0-0 - 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-3814 advisory.

---------- Debian LTS Advisory DLA-3814-1 debian-lts@lists.debian.org https://www.debian.org/lts/security/ Markus Koschany May 13, 2024 https://wiki.debian.org/LTS

Package : glib2.0 Version : 2.58.3-2+deb10u6 CVE ID : CVE-2024-34397

Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact.

For Debian 10 buster, this problem has been fixed in version 2.58.3-2+deb10u6.

We recommend that you upgrade your glib2.0 packages.

For the detailed security status of glib2.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/glib2.0

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/glib2.0
https://security-tracker.debian.org/tracker/CVE-2024-34397
https://packages.debian.org/source/buster/glib2.0

Solution

Upgrade the libglib2.0-0 packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-34397

Plugin Information

Published: 2024/05/14, Modified: 2025/06/19

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.58.3-2+deb10u3
Should be : libglib2.0-0_2.58.3-2+deb10u6
Remote package installed : libglib2.0-data_2.58.3-2+deb10u3
Should be : libglib2.0-data_2.58.3-2+deb10u6
```

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-3758 : libtiff-dev - security update: Upgrade the libtiff-dev packages.	47	1
Debian dla-3763 : curl - security update: Upgrade the curl packages.	24	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-3818 : apache2 - security update: Upgrade the apache2 packages.	18	1
Debian dla-3833 : libapache2-mod-php7.3 - security update: Upgrade the libapache2-mod-php7.3 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-3820 : bluetooth - security update: Upgrade the bluetooth packages.	12	1
Debian dla-3530 : libssl-dev - security update: Upgrade the libssl-dev packages.	11	1
Debian dla-3816 : bind9 - security update: Upgrade the bind9 packages.	10	1
Debian dla-3649 : python-urllib3 - security update: Upgrade the python-urllib3 packages.	8	1
Debian dla-3603 : libxpm-dev - security update: Upgrade the libxpm-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 dla-3750 : php-phpseclib - security update: Upgrade the php-phpseclib packages.	5	1
Debian dla-3814 : libglib2.0-0 - security update: Upgrade the libglib2.0-0 packages.	5	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-3781 : libgd-dev - security update: Upgrade the libgd-dev packages.	3	1
Debian dla-3804 : libnghttp2-14 - security update: Upgrade the libnghttp2-14 packages.	3	1
Debian dla-3101 : libxslt1-dev - security update: Upgrade the libxslt1-dev packages.	2	1
Debian dla-3103 : lib32z1 - security update: Upgrade the lib32z1 packages.	2	1
Debian dla-3118 : unzip - security update: Upgrade the unzip 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-3466 : avahi-autoipd - security update: Upgrade the avahi-autoipd packages.	2	1
Debian dla-3570 : libwebp-dev - security update: Upgrade the libwebp-dev packages.	2	1
Debian dla-3722 : libmariadb-dev - security update: Upgrade the libmariadb-dev 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-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-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-3456 : python-requests - security update: Upgrade the python-requests 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-3743 : hostapd - security update: Upgrade the hostapd packages.	1	1
Debian dla-3755 : tar - security update: Upgrade the tar packages.	1	1
Debian dla-3811 : pypy-idna - security update: Upgrade the pypy-idna 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