



Tiki

Tue, 04 Nov 2025 09:52:48 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.22.169.205

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

- Suggested Remediations

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

10.22.169.205

133

244

410

61

164

CRITICAL

HIGH

MEDIUM

LOW

INFO

Scan Information

Start time: Tue Nov 4 09:45:54 2025

End time: Tue Nov 4 09:52:47 2025

Host Information

Netbios Name: UBUNTU
IP: 10.22.169.205
MAC Address: 08:00:27:78:DD:49
OS: Linux Kernel 5.4.0-42-generic on Ubuntu 20.04

Vulnerabilities

201388 - Canonical Ubuntu Linux SEoL (20.04.x)

Synopsis

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

Description

According to its version, Canonical Ubuntu Linux is 20.04.x. It is, therefore, no longer maintained by its vendor or provider.

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

See Also

<https://wiki.ubuntu.com Releases>

Solution

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/0

```
OS : Canonical Ubuntu Linux 20.04.1 LTS (Focal Fossa)
Security End of Life : May 29, 2025
Time since Security End of Life (Est.) : >= 1 month
```

207058 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Setuptools vulnerability (USN-7002-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7002-1 advisory.

It was discovered that setuptools was vulnerable to remote code execution. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7002-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2024-6345 |
| XREF | USN:7002-1 |

Plugin Information

Published: 2024/09/12, Modified: 2024/09/12

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : python3-pkg-resources_45.2.0-1
- Fixed package : python3-pkg-resources_45.2.0-1ubuntu0.2

209121 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : libarchive vulnerabilities (USN-7070-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7070-1 advisory.

It was discovered that libarchive mishandled certain memory checks, which could result in a NULL pointer dereference. An attacker could potentially use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-36227)

It was discovered that libarchive mishandled certain memory operations, which could result in an out-of- bounds memory access. An attacker could potentially use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-48957, CVE-2024-48958)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7070-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-36227 |
| CVE | CVE-2024-48957 |
| CVE | CVE-2024-48958 |
| XREF | USN:7070-1 |
| XREF | IAVB:2024-B-0154-S |

Plugin Information

Published: 2024/10/16, Modified: 2025/03/19

Plugin Output

tcp/0

- Installed package : libarchive13_3.4.0-2ubuntu1
- Fixed package : libarchive13_3.4.0-2ubuntu1.3

214143 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : rsync vulnerabilities (USN-7206-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7206-1 advisory.

Simon Scannell, Pedro Gallegos, and Jasiel Spelman discovered that rsync did not properly handle checksum lengths. An attacker could use this issue to execute arbitrary code. (CVE-2024-12084)

Simon Scannell, Pedro Gallegos, and Jasiel Spelman discovered that rsync compared checksums with uninitialized memory. An attacker could exploit this issue to leak sensitive information. (CVE-2024-12085)

Simon Scannell, Pedro Gallegos, and Jasiel Spelman discovered that rsync incorrectly handled file checksums. A malicious server could use this to expose arbitrary client files. (CVE-2024-12086)

Simon Scannell, Pedro Gallegos, and Jasiel Spelman discovered that rsync mishandled symlinks for some settings. An attacker could exploit this to write files outside the intended directory. (CVE-2024-12087)

Simon Scannell, Pedro Gallegos, and Jasiel Spelman discovered that rsync failed to verify symbolic link destinations for some settings. An attacker could exploit this for path traversal attacks. (CVE-2024-12088)

Aleksei Gorban discovered a race condition in rsync's handling of symbolic links. An attacker could use this to access sensitive information or escalate privileges. (CVE-2024-12747)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7206-1>

Solution

Update the affected rsync package.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE

CVE-2024-12084

| | |
|------|----------------|
| CVE | CVE-2024-12085 |
| CVE | CVE-2024-12086 |
| CVE | CVE-2024-12087 |
| CVE | CVE-2024-12088 |
| CVE | CVE-2024-12747 |
| XREF | USN:7206-1 |

Plugin Information

Published: 2025/01/14, Modified: 2025/06/19

Plugin Output

tcp/0

- Installed package : rsync_3.1.3-8
- Fixed package : rsync_3.1.3-8ubuntu0.8

207059 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 24.04 LTS : Expat vulnerabilities (USN-7000-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7000-1 advisory.

Shang-Hung Wan discovered that Expat did not properly handle certain function calls when a negative input length was provided. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code. (CVE-2024-45490)

Shang-Hung Wan discovered that Expat did not properly handle the potential for an integer overflow on 32-bit platforms. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code. (CVE-2024-45491, CVE-2024-45492)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7000-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-45490 |
| CVE | CVE-2024-45491 |
| CVE | CVE-2024-45492 |
| XREF | USN:7000-1 |
| XREF | IAVA:2024-A-0543-S |

Plugin Information

Published: 2024/09/12, Modified: 2025/03/21

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.7

243224 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-7679-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7679-1 advisory.

It was discovered that SQLite incorrectly handled aggregate terms. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2025-6965)

It was discovered that SQLite incorrectly handled certain argument values to sqlite3_db_config(). An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. This update fixes the issue in Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS. This issue was previously fixed in Ubuntu 20.04 LTS via USN-7528-1. (CVE-2025-29088)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7679-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

7.2 (CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/NC:L/VI:H/VA:L/SC:L/SI:H/SA:L)

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2025-6965 |
| CVE | CVE-2025-29088 |
| XREF | IAVA:2025-A-0288-S |
| XREF | IAVA:2025-A-0529 |
| XREF | USN:7679-1 |

Plugin Information

Published: 2025/07/31, Modified: 2025/07/31

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.7+esm1

189748 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 : Ceph vulnerability (USN-6613-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6613-1 advisory.

Lucas Henry discovered that Ceph incorrectly handled specially crafted POST requests. An upprivileged user could use this to

bypass Ceph's authorization checks and upload a file to any bucket.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6613-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-43040 |
| XREF | USN:6613-1 |

Plugin Information

Published: 2024/01/29, Modified: 2025/08/15

Plugin Output

tcp/0

- Installed package : libcephfs2_15.2.3-0ubuntu0.20.04.1
- Fixed package : libcephfs2_15.2.17-0ubuntu0.20.04.6

- Installed package : librados2_15.2.3-0ubuntu0.20.04.1
- Fixed package : librados2_15.2.17-0ubuntu0.20.04.6

176501 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : snapd vulnerability (USN-6125-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6125-1 advisory.

It was discovered that the snap sandbox did not restrict the use of the ioctl system call with a TIOCLINUX request. This could be exploited by a malicious snap to inject commands into the controlling terminal which would then be executed outside of the snap sandbox once the snap had exited. This could allow an attacker to execute arbitrary commands outside of the confined snap sandbox. Note: graphical terminal emulators like xterm, gnome-terminal and others are not affected - this can only be exploited when snaps are run on a virtual console.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6125-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.0 (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-2023-1523 |
| XREF | USN:6125-1 |

Plugin Information

Published: 2023/05/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.58+20.04.1

174272 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerability (USN-6017-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6017-1 advisory.

Hadrien Perrineau discovered that Ghostscript incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6017-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-28879 |
| XREF | USN:6017-1 |
| XREF | IAVB:2023-B-0023-S |

Plugin Information

Published: 2023/04/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : `ghostscript_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript_9.50~dfsg-5ubuntu4.7`
- Installed package : `ghostscript-x_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript-x_9.50~dfsg-5ubuntu4.7`
- Installed package : `libgs9_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9_9.50~dfsg-5ubuntu4.7`
- Installed package : `libgs9-common_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9-common_9.50~dfsg-5ubuntu4.7`

166264 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5688-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5688-1 advisory.

It was discovered that an integer overflow could be triggered in Libksba when decoding certain data. An attacker could use this issue to cause a denial of service (application crash) or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5688-1>

Solution

Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2022-3515 |
| XREF | USN:5688-1 |
| XREF | IAVA:2023-A-0072 |

Plugin Information

Published: 2022/10/19, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libksba8_1.3.5-2
- Fixed package : libksba8_1.3.5-2ubuntu0.20.04.1

[171011 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM regressions \(USN-5825-2\)](#)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5825-2 advisory.

USN-5825-1 fixed vulnerabilities in PAM. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5825-2>

Solution

Update the affected 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:I/C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-28321 |
| XREF | USN:5825-2 |

Plugin Information

Published: 2023/02/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libpam-modules_1.3.1-5ubuntu4
- Fixed package : libpam-modules_1.3.1-5ubuntu4.6
- Installed package : libpam-modules-bin_1.3.1-5ubuntu4
- Fixed package : libpam-modules-bin_1.3.1-5ubuntu4.6
- Installed package : libpam-runtime_1.3.1-5ubuntu4
- Fixed package : libpam-runtime_1.3.1-5ubuntu4.6
- Installed package : libpam0g_1.3.1-5ubuntu4
- Fixed package : libpam0g_1.3.1-5ubuntu4.6

170644 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM vulnerability (USN-5825-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5825-1 advisory.

It was discovered that PAM did not correctly restrict login from an IP address that is not resolvable via DNS. An attacker could possibly use this issue to bypass authentication.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5825-1>

Solution

Update the affected 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
XREF
CVE-2022-28321
USN:5825-1

Plugin Information

Published: 2023/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpam-modules_1.3.1-5ubuntu4
- Fixed package : libpam-modules_1.3.1-5ubuntu4.4
- Installed package : libpam-modules-bin_1.3.1-5ubuntu4
- Fixed package : libpam-modules-bin_1.3.1-5ubuntu4.4
- Installed package : libpam-runtime_1.3.1-5ubuntu4
- Fixed package : libpam-runtime_1.3.1-5ubuntu4.4
- Installed package : libpam0g_1.3.1-5ubuntu4
- Fixed package : libpam0g_1.3.1-5ubuntu4.4

170001 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5800-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5800-1 advisory.

It was discovered that Heimdal incorrectly handled certain SPNEGO tokens. A remote attacker could possibly use this issue to cause a denial of service. (CVE-2021-44758)

Evgeny Legerov discovered that Heimdal incorrectly handled memory when performing certain DES decryption operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-3437)

Greg Hudson discovered that Kerberos PAC implementation used in Heimdal incorrectly handled certain parsing operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-42898)

It was discovered that Heimdal's KDC did not properly handle certain error conditions. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-44640)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5800-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-44758 |
| CVE | CVE-2022-3437 |
| CVE | CVE-2022-42898 |
| CVE | CVE-2022-44640 |
| XREF | USN:5800-1 |

Plugin Information

Published: 2023/01/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1.3
- Installed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1.3

164287 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5573-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5573-1 advisory.

Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate operations.

An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5573-1>

Solution

Update the affected rsync package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE-2022-37434
XREF USN:5573-1

Plugin Information

Published: 2022/08/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : rsync_3.1.3-8
- Fixed package : rsync_3.1.3-8ubuntu0.4

211522 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : GLib vulnerability (USN-7114-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7114-1 advisory.

It was discovered that Glib incorrectly handled certain trailing characters. An attacker could possibly use this issue to cause a crash or other undefined behavior.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7114-1>

Solution

Update the affected 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-2024-52533 |
| XREF | USN:7114-1 |
| XREF | IAVA:2024-A-0757-S |

Plugin Information

Published: 2024/11/18, Modified: 2025/06/17

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.8
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.8
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.8

182520 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : FreeRDP vulnerabilities (USN-6401-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6401-1 advisory.

It was discovered that FreeRDP did not properly manage certain inputs. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive

information. (CVE-2023-39350, CVE-2023-39351,

CVE-2023-39353,

CVE-2023-39354, CVE-2023-40181, CVE-2023-40188, CVE-2023-40589)

It was discovered that FreeRDP did not properly manage certain inputs. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-40186, CVE-2023-40567, CVE-2023-40569)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6401-1>

Solution

Update the affected 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-2023-39350 |
| CVE | CVE-2023-39351 |
| CVE | CVE-2023-39353 |
| CVE | CVE-2023-39354 |
| CVE | CVE-2023-40181 |
| CVE | CVE-2023-40186 |
| CVE | CVE-2023-40188 |
| CVE | CVE-2023-40567 |
| CVE | CVE-2023-40569 |
| CVE | CVE-2023-40589 |
| XREF | USN:6401-1 |

Plugin Information

Published: 2023/10/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.5
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.5
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.5

182769 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6420-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6420-1 advisory.

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3235, CVE-2022-3278, CVE-2022-3297, CVE-2022-3491)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3352, CVE-2022-4292)

It was discovered that Vim incorrectly handled memory when replacing in virtualedit mode. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3234)

It was discovered that Vim incorrectly handled memory when autocmd changes mark. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3256)

It was discovered that Vim did not properly perform checks on array index with negative width window. An attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2022-3324)

It was discovered that Vim did not properly perform checks on a put command column with a visual block. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3520)

It was discovered that Vim incorrectly handled memory when using autocommand to open a window. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3591)

It was discovered that Vim incorrectly handled memory when updating buffer of the component autocmd handler. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3705)

It was discovered that Vim incorrectly handled floating point comparison with incorrect operator. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-4293)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6420-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-3234 |
| CVE | CVE-2022-3235 |
| CVE | CVE-2022-3256 |
| CVE | CVE-2022-3278 |
| CVE | CVE-2022-3297 |
| CVE | CVE-2022-3324 |
| CVE | CVE-2022-3352 |
| CVE | CVE-2022-3491 |
| CVE | CVE-2022-3520 |
| CVE | CVE-2022-3591 |
| CVE | CVE-2022-3705 |
| CVE | CVE-2022-4292 |
| CVE | CVE-2022-4293 |
| XREF | IAVB:2022-B-0049-S |
| XREF | IAVB:2022-B-0058-S |
| XREF | IAVB:2023-B-0016-S |
| XREF | USN:6420-1 |

Plugin Information

Published: 2023/10/09, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.18
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.18
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.18

175722 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6075-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6075-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215)

Irvan Kurniawan discovered that Thunderbird did not properly manage memory when using RLBox Expat driver.
An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6075-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-32205 |
| CVE | CVE-2023-32206 |
| CVE | CVE-2023-32207 |
| CVE | CVE-2023-32211 |
| CVE | CVE-2023-32212 |
| CVE | CVE-2023-32213 |
| CVE | CVE-2023-32215 |
| XREF | USN:6075-1 |
| XREF | IAVA:2023-A-0255-S |

Plugin Information

Published: 2023/05/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.11.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.11.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1

- Fixed package : thunderbird-locale-de_1:102.11.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.11.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.11.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.11.0+build1-0ubuntu0.20.04.1

172444 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5942-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5942-1 advisory.

Lars Krapf discovered that the Apache HTTP Server mod_proxy module incorrectly handled certain configurations. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2023-25690)

Dimas Fariski Setyawan Putra discovered that the Apache HTTP Server mod_proxy_uwsgi module incorrectly handled certain special characters. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-27522)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5942-1>

Solution

Update the affected 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: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 | USN:5942-1 |
| XREF | IAVA:2023-A-0124-S |

Plugin Information

Published: 2023/03/10, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.14

- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.14

- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.14

- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.14
```

237431 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU C Library vulnerability (USN-7541-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7541-1 advisory.

It was discovered that the GNU C Library incorrectly search LD_LIBRARY_PATH to determine which library to load when statically linked setuid binary calls dlopen. A local attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7541-1>

Solution

Update the affected packages.

Risk Factor

Critical

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

6.8 (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)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-4802 |
| XREF | IAVA:2025-A-0062 |
| XREF | USN:7541-1 |

Plugin Information

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

Plugin Output

tcp/0

```
- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.18
```

- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.18
- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.18
- Installed package : libc6-dev_2.31-0ubuntu9
- Fixed package : libc6-dev_2.31-0ubuntu9.18
- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.18

168337 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerability (USN-5743-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5743-2 advisory.

USN-5743-1 fixed a vulnerability in LibTIFF. This update provides the corresponding updates for Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5743-2>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2022-3970 |
| XREF | USN:5743-2 |

Plugin Information

Published: 2022/12/02, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.7

169583 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5787-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5787-1 advisory.

It was discovered that Libksba incorrectly handled parsing CRL signatures. A remote attacker could use this issue to cause Libksba to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5787-1>

Solution

Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-47629 |
| XREF | USN:5787-1 |
| XREF | IAVA:2023-A-0072 |

Plugin Information

Published: 2023/01/05, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libksba8_1.3.5-2
- Fixed package : libksba8_1.3.5-2ubuntu0.20.04.2
```

170565 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5823-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5823-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.32 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. Ubuntu 18.04 LTS has been updated to MySQL 5.7.41.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-41.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-32.html>
<https://www.oracle.com/security-alerts/cpujan2023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5823-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-32221 |
| CVE | CVE-2023-21836 |
| CVE | CVE-2023-21840 |
| CVE | CVE-2023-21863 |
| CVE | CVE-2023-21867 |
| CVE | CVE-2023-21868 |
| CVE | CVE-2023-21869 |
| CVE | CVE-2023-21870 |
| CVE | CVE-2023-21871 |
| CVE | CVE-2023-21873 |
| CVE | CVE-2023-21875 |
| CVE | CVE-2023-21876 |
| CVE | CVE-2023-21877 |
| CVE | CVE-2023-21878 |
| CVE | CVE-2023-21879 |
| CVE | CVE-2023-21880 |
| CVE | CVE-2023-21881 |
| CVE | CVE-2023-21882 |
| CVE | CVE-2023-21883 |
| CVE | CVE-2023-21887 |
| XREF | USN:5823-1 |

Plugin Information

Published: 2023/01/25, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.32-0ubuntu0.20.04.1

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5506-1 advisory.

Tavis Ormandy discovered that NSS incorrectly handled an empty pkcs7 sequence. A remote attacker could possibly use this issue to cause NSS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-22747)

Ronald Crane discovered that NSS incorrectly handled certain memory operations. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-34480)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5506-1>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-22747 |
| CVE | CVE-2022-34480 |
| XREF | USN:5506-1 |

Plugin Information

Published: 2022/07/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.8

171951 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NSS vulnerabilities (USN-5892-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5892-1 advisory.

It was discovered that NSS incorrectly handled client authentication without a user certificate in the database. A remote attacker could possibly use this issue to cause a NSS client to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-3479)

Christian Holler discovered that NSS incorrectly handled certain PKCS 12 certificated bundles. A remote attacker could use this issue to cause NSS to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-0767)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5892-1>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2022-3479 |
| CVE | CVE-2023-0767 |
| XREF | USN:5892-1 |

Plugin Information

Published: 2023/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.9

168516 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-5767-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5767-1 advisory.

Nicky Mouha discovered that Python incorrectly handled certain SHA-3 internals. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-37454)

It was discovered that Python incorrectly handled certain IDNA inputs. An attacker could possibly use this issue to expose sensitive information denial of service, or cause a crash. (CVE-2022-45061)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5767-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2022-37454 |
| CVE | CVE-2022-45061 |
| XREF | USN:5767-1 |
| XREF | IAVA:2023-A-0061-S |

Plugin Information

Published: 2022/12/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.6
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.6
- Installed package : libpython3.8-stplib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stplib_3.8.10-0ubuntu1~20.04.6
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.6
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.6

[161448 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities \(USN-5435-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5435-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass permission prompts, obtain sensitive information, bypass security restrictions, cause user confusion, or execute arbitrary code. (CVE-2022-29909, CVE-2022-29911, CVE-2022-29912, CVE-2022-29913, CVE-2022-29914, CVE-2022-29916, CVE-2022-29917)

It was discovered that Thunderbird would show the wrong security status after viewing an attached message that is signed or encrypted. An attacker could potentially exploit this by tricking the user into trusting the authenticity of a message. (CVE-2022-1520)

It was discovered that the methods of an Array object could be corrupted as a result of prototype pollution by sending a message to the parent process. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could exploit this to execute JavaScript in a privileged context. (CVE-2022-

1529, CVE-2022-1802)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5435-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1520 |
| CVE | CVE-2022-1529 |
| CVE | CVE-2022-1802 |
| CVE | CVE-2022-29909 |
| CVE | CVE-2022-29911 |
| CVE | CVE-2022-29912 |
| CVE | CVE-2022-29913 |
| CVE | CVE-2022-29914 |
| CVE | CVE-2022-29916 |
| CVE | CVE-2022-29917 |
| XREF | USN:5435-1 |
| XREF | IAVA:2022-A-0217-S |

Plugin Information

Published: 2022/05/24, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:91.9.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:91.9.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:91.9.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:91.9.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:91.9.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:91.9.1+build1-0ubuntu0.20.04.1

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5512-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass CSP restrictions, or execute arbitrary code.
(CVE-2022-2200, CVE-2022-31736, CVE-2022-31737, CVE-2022-31738, CVE-2022-31740, CVE-2022-31741, CVE-2022-31742, CVE-2022-31744, CVE-2022-31747, CVE-2022-34468, CVE-2022-34470, CVE-2022-34479, CVE-2022-34481, CVE-2022-34484)

It was discovered that an unavailable PAC file caused OCSP requests to be blocked, resulting in incorrect error pages being displayed. (CVE-2022-34472)

It was discovered that the Braille space character could be used to cause Thunderbird to display the wrong sender address for signed messages. An attacker could potentially exploit this to trick the user into believing a message had been sent from somebody they trusted. (CVE-2022-1834)

It was discovered that Thunderbird would consider an email with a mismatched OpenPGP signature date as valid. An attacker could potentially exploit this by replaying an older message in order to trick the user into believing that the statements in the message are current. (CVE-2022-2226)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5512-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1834 |
| CVE | CVE-2022-2200 |
| CVE | CVE-2022-2226 |
| CVE | CVE-2022-31736 |
| CVE | CVE-2022-31737 |
| CVE | CVE-2022-31738 |
| CVE | CVE-2022-31740 |
| CVE | CVE-2022-31741 |
| CVE | CVE-2022-31742 |
| CVE | CVE-2022-31744 |
| CVE | CVE-2022-31747 |
| CVE | CVE-2022-34468 |
| CVE | CVE-2022-34470 |
| CVE | CVE-2022-34472 |
| CVE | CVE-2022-34479 |
| CVE | CVE-2022-34481 |
| CVE | CVE-2022-34484 |
| XREF | USN:5512-1 |
| XREF | IAVA:2022-A-0226-S |
| XREF | IAVA:2022-A-0256-S |

Plugin Information

Published: 2022/07/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:91.11.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:91.11.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:91.11.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:91.11.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:91.11.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:91.11.0+build2-0ubuntu0.20.04.1
```

165820 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-5663-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5663-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service,

spoof the mouse pointer position, obtain sensitive information, spoof the contents of the addressbar, bypass security restrictions, or execute arbitrary code. (CVE-2022-2505, CVE-2022-36318, CVE-2022-36319, CVE-2022-38472, CVE-2022-38473, CVE-2022-38476 CVE-2022-38477, CVE-2022-38478)

Multiple security issues were discovered in Thunderbird. An attacker could potentially exploit these in order to determine when a user opens a specially crafted message. (CVE-2022-3032, CVE-2022-3034)

It was discovered that Thunderbird did not correctly handle HTML messages that contain a meta tag in some circumstances. If a user were tricked into replying to a specially crafted message, an attacker could potentially exploit this to obtain sensitive information. (CVE-2022-3033)

A security issue was discovered with the Matrix SDK in Thunderbird. An attacker sharing a room with a user could potentially exploit this to cause a denial of service. (CVE-2022-36059)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5663-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-2505 |
| CVE | CVE-2022-3032 |
| CVE | CVE-2022-3033 |
| CVE | CVE-2022-3034 |
| CVE | CVE-2022-36059 |
| CVE | CVE-2022-36318 |
| CVE | CVE-2022-36319 |
| CVE | CVE-2022-38472 |
| CVE | CVE-2022-38473 |
| CVE | CVE-2022-38476 |
| CVE | CVE-2022-38477 |
| CVE | CVE-2022-38478 |
| XREF | USN:5663-1 |
| XREF | IAVA:2022-A-0342-S |
| XREF | IAVA:2022-A-0349-S |

Plugin Information

Published: 2022/10/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.2.2+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.2.2+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.2.2+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.2.2+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.2.2+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.2.2+build1-0ubuntu0.20.04.1

167286 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-5724-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5724-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass Content Security Policy (CSP) or other security restrictions, or execute arbitrary code. These issues only affect Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3266, CVE-2022-40956, CVE-2022-40957, CVE-2022-40958, CVE-2022-40959, CVE-2022-40960, CVE-2022-40962)

Multiple security issues were discovered in the Matrix SDK bundled with Thunderbird. An attacker could potentially exploit these in order to impersonate another user. These issues only affect Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-39236, CVE-2022-39249, CVE-2022-39250, CVE-2022-39251)

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42932)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5724-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-3266 |
| CVE | CVE-2022-39236 |
| CVE | CVE-2022-39249 |
| CVE | CVE-2022-39250 |
| CVE | CVE-2022-39251 |
| CVE | CVE-2022-40956 |
| CVE | CVE-2022-40957 |
| CVE | CVE-2022-40958 |
| CVE | CVE-2022-40959 |
| CVE | CVE-2022-40960 |
| CVE | CVE-2022-40962 |
| CVE | CVE-2022-42927 |
| CVE | CVE-2022-42928 |
| CVE | CVE-2022-42929 |
| CVE | CVE-2022-42932 |
| XREF | USN:5724-1 |
| XREF | IAVA:2022-A-0386-S |
| XREF | IAVA:2022-A-0393-S |
| XREF | IAVA:2022-A-0444-S |

Plugin Information

Published: 2022/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.4.2+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.4.2+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.4.2+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.4.2+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.4.2+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.4.2+build2-0ubuntu0.20.04.1

171009 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-5824-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5824-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45418, CVE-2022-45420, CVE-2022-45421, CVE-2022-46878, CVE-2022-46880, CVE-2022-46881, CVE-2022-46882, CVE-2023-23605)

Armin Ebert discovered that Thunderbird did not properly manage memory while resolving file symlink. If a user were tricked into opening a specially crafted weblink, an attacker could potentially exploit these to cause a denial of service. (CVE-2022-45412)

Sarah Jamie Lewis discovered that Thunderbird did not properly manage network request while handling HTML emails with certain tags. If a user were tricked into opening a specially HTML email, an attacker could potentially exploit these issue and load remote content regardless of a configuration to block remote content. (CVE-2022-45414)

Erik Kraft, Martin Schwarzl, and Andrew McCreight discovered that Thunderbird incorrectly handled keyboard events. An attacker could possibly use this issue to perform a timing side-channel attack and possibly figure out which keys are being pressed. (CVE-2022-45416)

It was discovered that Thunderbird was using an out-of-date libusrscpt library. An attacker could possibly use this library to perform a reentrancy issue on Thunderbird. (CVE-2022-46871)

Nika Layzell discovered that Thunderbird was not performing a check on paste received from cross- processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)

Matthias Zoellner discovered that Thunderbird was not keeping the filename ending intact when using the drag-and-drop event. An attacker could possibly use this issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)

Hafizh discovered that Thunderbird was not properly handling fullscreen notifications when the window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)

Tom Schuster discovered that Thunderbird was not performing a validation check on GTK drag data. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23598)

Vadim discovered that Thunderbird was not properly sanitizing a curl command output when copying a network request from the developer tools panel. An attacker could potentially exploits this to hide and execute arbitrary commands. (CVE-2023-23599)

Luan Herrera discovered that Thunderbird was not stopping navigation when dragging a URL from a cross- origin iframe into the same tab. An attacker potentially exploits this to spoof the user. (CVE-2023-23601)

Dave Vandyke discovered that Thunderbird did not properly implement CSP policy when creating a WebSocket in a WebWorker. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2023-23602)

Dan Veditz discovered that Thunderbird did not properly implement CSP policy on regular expression when using console.log. An attacker potentially exploits this to exfiltrate data. (CVE-2023-23603)

It was discovered that Thunderbird did not properly check the Certificate OCSP revocation status when verifying S/Mime signatures. An attacker could possibly use this issue to bypass signature validation check by sending email signed with a revoked certificate. (CVE-2023-0430)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5824-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-45403 |
| CVE | CVE-2022-45404 |
| CVE | CVE-2022-45405 |
| CVE | CVE-2022-45406 |
| CVE | CVE-2022-45408 |
| CVE | CVE-2022-45409 |
| CVE | CVE-2022-45410 |
| CVE | CVE-2022-45411 |
| CVE | CVE-2022-45412 |
| CVE | CVE-2022-45414 |
| CVE | CVE-2022-45416 |
| CVE | CVE-2022-45418 |
| CVE | CVE-2022-45420 |
| CVE | CVE-2022-45421 |
| CVE | CVE-2022-46871 |
| CVE | CVE-2022-46872 |
| CVE | CVE-2022-46874 |
| CVE | CVE-2022-46877 |
| CVE | CVE-2022-46878 |
| CVE | CVE-2022-46880 |
| CVE | CVE-2022-46881 |
| CVE | CVE-2022-46882 |
| CVE | CVE-2023-0430 |
| CVE | CVE-2023-23598 |
| CVE | CVE-2023-23599 |
| CVE | CVE-2023-23601 |
| CVE | CVE-2023-23602 |
| CVE | CVE-2023-23603 |
| CVE | CVE-2023-23605 |
| XREF | USN:5824-1 |
| XREF | IAVA:2023-A-0056-S |
| XREF | IAVA:2022-A-0519-S |
| XREF | IAVA:2022-A-0492-S |
| XREF | IAVA:2022-A-0505-S |
| XREF | IAVA:2023-A-0009-S |

Plugin Information

Published: 2023/02/06, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.7.1+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.7.1+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.7.1+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.7.1+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.7.1+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.7.1+build2-0ubuntu0.20.04.1
```

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5943-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-0616, CVE-2023-25735, CVE-2023-25737, CVE-2023-25739, CVE-2023-25729, CVE-2023-25742, CVE-2023-25746)

Johan Carlsson discovered that Thunderbird did not properly implement CSP policy on a header when using iframes. An attacker could potentially exploits this to exfiltrate data. (CVE-2023-25728)

Irvan Kurniawan discovered that Thunderbird was not properly handling background fullscreen scripts when the window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2023-25730)

Christian Holler discovered that Thunderbird did not properly check the Safe Bag attributes in PKCS 12 certificate bundle. An attacker could possibly use this issue to write to arbitrary memory by sending malicious PKCS 12 certificate. (CVE-2023-0767)

Ronald Crane discovered that Thunderbird did not properly check the size of the input being encoded in xpcom. An attacker could possibly use this issue to perform out of bound memory write operations. (CVE-2023-25732)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5943-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-0616 |
| CVE | CVE-2023-0767 |
| CVE | CVE-2023-25728 |
| CVE | CVE-2023-25729 |
| CVE | CVE-2023-25730 |
| CVE | CVE-2023-25732 |
| CVE | CVE-2023-25735 |
| CVE | CVE-2023-25737 |
| CVE | CVE-2023-25739 |
| CVE | CVE-2023-25742 |
| CVE | CVE-2023-25746 |
| XREF | USN:5943-1 |
| XREF | IAVA:2023-A-0106-S |

Plugin Information

Published: 2023/03/13, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.8.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.8.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.8.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.8.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.8.0+build2-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.8.0+build2-0ubuntu0.20.04.1
```

173424 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-5972-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5972-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-25152, CVE-2023-28162, CVE-2023-28176)

Lukas Bernhard discovered that Thunderbird did not properly manage memory when invalidating JIT code while following an iterator. An attacker could potentially exploits this issue to cause a denial of service.

(CVE-2023-25751)

Luan Herrera discovered that Thunderbird did not properly manage cross-origin iframe when dragging a URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-28164)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5972-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2023-25751 |
| CVE | CVE-2023-25752 |
| CVE | CVE-2023-28162 |
| CVE | CVE-2023-28164 |
| CVE | CVE-2023-28176 |
| XREF | USN:5972-1 |
| XREF | IAVA:2023-A-0149-S |

Plugin Information

Published: 2023/03/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.9.0+build1-0ubuntu0.20.04.1

174266 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-6015-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6015-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-1945, CVE-2023-29548, CVE-2023-29550)

Paul Menzel discovered that Thunderbird did not properly validate OCSP revocation status of recipient certificates when sending S/Mime encrypted email. An attacker could potentially exploits this issue to perform spoofing attack. (CVE-2023-0547)

Ribose RNP Team discovered that Thunderbird did not properly manage memory when parsing certain OpenPGP messages. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29479)

Irvan Kurniawan discovered that Thunderbird did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)

Lukas Bernhard discovered that Thunderbird did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service.
(CVE-2023-29535)

Zx from qriousec discovered that Thunderbird did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29536)

Trung Pham discovered that Thunderbird did not properly validate the filename directive in the Content- Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)

Ameen Basha M K discovered that Thunderbird did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6015-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-0547 |
| CVE | CVE-2023-1945 |
| CVE | CVE-2023-29479 |
| CVE | CVE-2023-29533 |
| CVE | CVE-2023-29535 |
| CVE | CVE-2023-29536 |
| CVE | CVE-2023-29539 |
| CVE | CVE-2023-29541 |
| CVE | CVE-2023-29548 |
| CVE | CVE-2023-29550 |
| XREF | USN:6015-1 |
| XREF | IAVA:2023-A-0199-S |

Plugin Information

Published: 2023/04/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.10.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.10.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.10.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.10.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.10.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.10.0+build2-0ubuntu0.20.04.1

166561 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5702-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5702-1 advisory.

Robby Simpson discovered that curl incorrectly handled certain POST operations after PUT operations. This issue could cause applications using curl to send the wrong data, perform incorrect memory operations, or crash. (CVE-2022-32221)

Hiroki Kurosawa discovered that curl incorrectly handled parsing .netrc files. If an attacker were able to provide a specially crafted .netrc file, this issue could cause curl to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-35260)

It was discovered that curl incorrectly handled certain HTTP proxy return codes. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-42915)

Hiroki Kurosawa discovered that curl incorrectly handled HSTS support when certain hostnames included IDN characters. A remote attacker could possibly use this issue to cause curl to use unencrypted connections.

This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-42916)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5702-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|------------------------------------|
| CVE | CVE-2022-32221 |
| CVE | CVE-2022-35260 |
| CVE | CVE-2022-42915 |
| CVE | CVE-2022-42916 |
| XREF | USN:5702-1 |
| XREF | IAVA:2022-A-0451-S |

Plugin Information

Published: 2022/10/26, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.14
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.14

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5964-1 advisory.

Harry Sintonen discovered that curl incorrectly handled certain TELNET connection options. Due to lack of proper input scrubbing, curl could pass on user name and telnet options to the server as provided, contrary to expectations. (CVE-2023-27533)

Harry Sintonen discovered that curl incorrectly handled special tilde characters when used with SFTP paths. A remote attacker could possibly use this issue to circumvent filtering. (CVE-2023-27534)

Harry Sintonen discovered that curl incorrectly reused certain FTP connections. This could lead to the wrong credentials being reused, contrary to expectations. (CVE-2023-27535)

Harry Sintonen discovered that curl incorrectly reused connections when the GSS delegation option had been changed. This could lead to the option being reused, contrary to expectations. (CVE-2023-27536)

Harry Sintonen discovered that curl incorrectly reused certain SSH connections. This could lead to the wrong credentials being reused, contrary to expectations. (CVE-2023-27538)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5964-1>

Solution

Update the affected packages.

Risk Factor

Critical

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

10.0 (CVSS2#AV:N/AC:L/Au:N/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-2023-27534 |
| CVE | CVE-2023-27535 |
| CVE | CVE-2023-27536 |
| CVE | CVE-2023-27538 |
| XREF | USN:5964-1 |
| XREF | IAVA:2023-A-0153-S |

Plugin Information

Published: 2023/03/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.18

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.18

167196 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : pixman vulnerability (USN-5718-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5718-1 advisory.

Maddie Stone discovered that pixman incorrectly handled certain memory operations. A remote attacker could use this issue to cause pixman to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5718-1>

Solution

Update the affected libpixman-1-0 and / or libpixman-1-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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-44638 |
| XREF | USN:5718-1 |

Plugin Information

Published: 2022/11/09, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libpixman-1-0_0.38.4-0ubuntu1
- Fixed package : libpixman-1-0_0.38.4-0ubuntu2.1

156744 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5229-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5229-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to

cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information across domains, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5229-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/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-2021-4140 |
| CVE | CVE-2022-22737 |
| CVE | CVE-2022-22738 |
| CVE | CVE-2022-22739 |
| CVE | CVE-2022-22740 |
| CVE | CVE-2022-22741 |
| CVE | CVE-2022-22742 |
| CVE | CVE-2022-22743 |
| CVE | CVE-2022-22745 |
| CVE | CVE-2022-22747 |
| CVE | CVE-2022-22748 |
| CVE | CVE-2022-22751 |
| CVE | CVE-2022-22752 |
| XREF | USN:5229-1 |
| XREF | IAVA:2022-A-0017-S |

Plugin Information

Published: 2022/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_96.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_96.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_96.0+build2-0ubuntu0.20.04.1

158053 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5284-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5284-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, obtain sensitive information, or execute arbitrary code. (CVE-2022-0511, CVE-2022-22755, CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22764)

It was discovered that extensions of a particular type could auto-update themselves and bypass the prompt that requests permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to bypass security restrictions. (CVE-2022-22754)

It was discovered that dragging and dropping an image into a folder could result in it being marked as executable. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to execute arbitrary code. (CVE-2022-22756)

It was discovered that Remote Agent, used in WebDriver, did not validate Host or Origin headers. If a user were tricked into opening a specially crafted website with WebDriver enabled, an attacker could potentially exploit this to connect back to the user's browser in order to control it. (CVE-2022-22757)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5284-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.6 (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-2022-0511 |
| CVE | CVE-2022-22754 |
| CVE | CVE-2022-22755 |
| CVE | CVE-2022-22756 |
| CVE | CVE-2022-22757 |
| CVE | CVE-2022-22759 |
| CVE | CVE-2022-22760 |
| CVE | CVE-2022-22761 |
| CVE | CVE-2022-22764 |
| XREF | USN:5284-1 |
| XREF | IAVA:2022-A-0079-S |

Plugin Information

Published: 2022/02/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_97.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_97.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_97.0.2+build1-0ubuntu0.20.04.1

158646 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5314-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5314-1 advisory.

A use-after-free was discovered when removing an XSLT parameter in some circumstances. If a user were tricked into opening a specially crafted website, an attacker could exploit this to cause a denial of service, or execute arbitrary code. (CVE-2022-26485)

A use-after-free was discovered in the WebGPU IPC framework. If a user were tricked into opening a specially crafted website, an attacker could exploit this to cause a denial of service, or execute arbitrary code. (CVE-2022-26486)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5314-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.9 (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)

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2022-26485 |
| CVE | CVE-2022-26486 |
| XREF | USN:5314-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/03/21 |
| XREF | IAVA:2022-A-0103-S |

Plugin Information

Published: 2022/03/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_97.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_97.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_97.0.2+build1-0ubuntu0.20.04.1

158817 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5321-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5321-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information, or execute arbitrary code.
(CVE-2022-0843, CVE-2022-26381, CVE-2022-26382, CVE-2022-26383, CVE-2022-26384, CVE-2022-26385)

A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature.

(CVE-2022-26387)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5321-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-0843 |
| CVE | CVE-2022-26381 |
| CVE | CVE-2022-26382 |
| CVE | CVE-2022-26383 |
| CVE | CVE-2022-26384 |
| CVE | CVE-2022-26385 |
| CVE | CVE-2022-26387 |
| XREF | USN:5321-1 |
| XREF | IAVA:2022-A-0103-S |

Plugin Information

Published: 2022/03/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1

- Fixed package : firefox_98.0+build3-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_98.0+build3-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_98.0+build3-0ubuntu0.20.04.2

159022 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5321-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5321-2 advisory.

USN-5321-1 fixed vulnerabilities in Firefox. The update didn't include arm64 because of a regression. This update provides the corresponding update for arm64.

This update also removes Yandex and Mail.ru as optional search providers in the drop-down search menu.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5321-2>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.6 (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-2022-0843 |
| CVE | CVE-2022-26381 |
| CVE | CVE-2022-26382 |
| CVE | CVE-2022-26383 |
| CVE | CVE-2022-26384 |
| CVE | CVE-2022-26385 |
| CVE | CVE-2022-26387 |
| XREF | USN:5321-2 |
| XREF | IAVA:2022-A-0103-S |

Plugin Information

Published: 2022/03/17, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_98.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_98.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_98.0.1+build2-0ubuntu0.20.04.1

161059 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5411-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5411-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass permission prompts, obtain sensitive information, bypass security restrictions, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5411-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-29909 |
| CVE | CVE-2022-29911 |
| CVE | CVE-2022-29912 |
| CVE | CVE-2022-29914 |
| CVE | CVE-2022-29915 |
| CVE | CVE-2022-29916 |
| CVE | CVE-2022-29917 |
| CVE | CVE-2022-29918 |
| XREF | USN:5411-1 |
| XREF | IAVA:2022-A-0188-S |

Plugin Information

Published: 2022/05/11, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_100.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_100.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_100.0+build2-0ubuntu0.20.04.1
```

161451 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5434-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5434-1 advisory.

It was discovered that the methods of an Array object could be corrupted as a result of prototype pollution by sending a message to the parent process. If a user were tricked into opening a specially crafted website, an attacker could exploit this to execute JavaScript in a privileged context.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5434-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1529 |
| CVE | CVE-2022-1802 |
| XREF | USN:5434-1 |
| KREF | IAVA:2022-A-0217-S |

Plugin Information

Published: 2022/05/24, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_100.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_100.0+build2-0ubuntu0.20.04.1
```

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_100.0.2+build1-0ubuntu0.20.04.1

162170 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5475-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5475-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the browser UI, conduct cross-site scripting (XSS) attacks, bypass content security policy (CSP) restrictions, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5475-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1919 |
| CVE | CVE-2022-31736 |
| CVE | CVE-2022-31737 |
| CVE | CVE-2022-31738 |
| CVE | CVE-2022-31740 |
| CVE | CVE-2022-31741 |
| CVE | CVE-2022-31742 |
| CVE | CVE-2022-31743 |
| CVE | CVE-2022-31744 |
| CVE | CVE-2022-31745 |
| CVE | CVE-2022-31747 |
| CVE | CVE-2022-31748 |
| XREF | USN:5475-1 |
| XREF | IAVA:2022-A-0226-S |
| XREF | IAVA:2022-A-0256-S |

Plugin Information

Published: 2022/06/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_101.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_101.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_101.0.1+build1-0ubuntu0.20.04.1

162735 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5504-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5504-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass CSP restrictions, bypass sandboxed iframe restrictions, obtain sensitive information, bypass the HTML sanitizer, or execute arbitrary code. (CVE-2022-2200, CVE-2022-34468, CVE-2022-34470, CVE-2022-34473, CVE-2022-34474, CVE-2022-34475, CVE-2022-34476, CVE-2022-34477, CVE-2022-34479, CVE-2022-34480, CVE-2022-34481, CVE-2022-34484, CVE-2022-34485)

It was discovered that Firefox could be made to save an image with an executable extension in the filename when dragging and dropping an image in some circumstances. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to trick the user into executing arbitrary code. (CVE-2022-34482, CVE-2022-34483)

It was discovered that a compromised server could trick Firefox into an addon downgrade in some circumstances. An attacker could potentially exploit this to trick the browser into downgrading an addon to a prior version. (CVE-2022-34471)

It was discovered that an unavailable PAC file caused OCSP requests to be blocked, resulting in incorrect error pages being displayed. (CVE-2022-34472)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5504-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|--------------------------------|
| CVE | CVE-2022-2200 |
| CVE | CVE-2022-34468 |
| CVE | CVE-2022-34470 |
| CVE | CVE-2022-34471 |
| CVE | CVE-2022-34472 |
| CVE | CVE-2022-34473 |

| | |
|------|--------------------|
| CVE | CVE-2022-34474 |
| CVE | CVE-2022-34475 |
| CVE | CVE-2022-34476 |
| CVE | CVE-2022-34477 |
| CVE | CVE-2022-34479 |
| CVE | CVE-2022-34480 |
| CVE | CVE-2022-34481 |
| CVE | CVE-2022-34482 |
| CVE | CVE-2022-34483 |
| CVE | CVE-2022-34484 |
| CVE | CVE-2022-34485 |
| XREF | USN:5504-1 |
| XREF | IAVA:2022-A-0256-S |

Plugin Information

Published: 2022/07/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_102.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_102.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_102.0+build2-0ubuntu0.20.04.1
```

163521 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5536-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5536-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the mouse pointer position, bypass Subresource Integrity protections, obtain sensitive information, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5536-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-2505 |
| CVE | CVE-2022-36315 |
| CVE | CVE-2022-36316 |
| CVE | CVE-2022-36318 |
| CVE | CVE-2022-36319 |
| CVE | CVE-2022-36320 |
| XREF | USN:5536-1 |
| XREF | IAVA:2022-A-0298-S |

Plugin Information

Published: 2022/07/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_103.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_103.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_103.0+build1-0ubuntu0.20.04.1

164392 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5581-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5581-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the contents of the addressbar, bypass security restrictions, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5581-1>

Solution

Update the affected 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

7.7 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-38472 |
| CVE | CVE-2022-38473 |
| CVE | CVE-2022-38475 |
| CVE | CVE-2022-38477 |
| CVE | CVE-2022-38478 |
| XREF | USN:5581-1 |
| XREF | IAVA:2022-A-0339-S |

Plugin Information

Published: 2022/08/24, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_104.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_104.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_104.0+build3-0ubuntu0.20.04.1

165601 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5649-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5649-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass Content Security Policy (CSP) or other security restrictions, conduct session fixation attacks, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5649-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|----------------|
| CVE | CVE-2022-3266 |
| CVE | CVE-2022-40956 |
| CVE | CVE-2022-40957 |

| | |
|------|--------------------|
| CVE | CVE-2022-40958 |
| CVE | CVE-2022-40959 |
| CVE | CVE-2022-40960 |
| CVE | CVE-2022-40962 |
| XREF | USN:5649-1 |
| XREF | IAVA:2022-A-0384-S |

Plugin Information

Published: 2022/09/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_105.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_105.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_105.0+build2-0ubuntu0.20.04.1

166800 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5709-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5709-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42930, CVE-2022-42932)

It was discovered that Firefox saved usernames to a plaintext file. A local user could potentially exploit this to obtain sensitive information. (CVE-2022-42931)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5709-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE

[CVE-2022-42927](#)

| | |
|------|--------------------|
| CVE | CVE-2022-42928 |
| CVE | CVE-2022-42929 |
| CVE | CVE-2022-42930 |
| CVE | CVE-2022-42931 |
| CVE | CVE-2022-42932 |
| XREF | USN:5709-1 |
| XREF | IAVA:2022-A-0435-S |
| XREF | IAVA:2023-A-0132-S |

Plugin Information

Published: 2022/11/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_106.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_106.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_106.0.2+build1-0ubuntu0.20.04.1

167744 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5726-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5726-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked

into opening a specially crafted website, an attacker could potentially

exploit these to cause a denial of service, spoof the contents of the addressbar, bypass security restrictions, cross-site tracing or execute arbitrary code. (CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45407, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45413, CVE-2022-40674, CVE-2022-45418, CVE-2022-45419, CVE-2022-45420, CVE-2022-45421)

Armin Ebert discovered that Firefox did not properly manage while resolving file symlink. If a user were tricked into opening a specially crafted weblink, an attacker could potentially exploit these to cause a denial of service.

(CVE-2022-45412)

Jefferson Scher and Jayateertha Guruprasad discovered that Firefox did not properly sanitize the HTML download file extension under certain circumstances. If a user were tricked into downloading and executing malicious content, a remote attacker could execute arbitrary code with the privileges of the user invoking the programs. (CVE-2022-45415)

Erik Kraft, Martin Schwarzl, and Andrew McCreight discovered that Firefox incorrectly handled keyboard events. An attacker could possibly use this issue to perform a timing side-channel attack and possibly figure out which keys are being pressed. (CVE-2022-45416)

Kagami discovered that Firefox did not detect Private Browsing Mode correctly. An attacker could possibly use this issue to obtain sensitive information about Private Browsing Mode. (CVE-2022-45417)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5726-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-40674 |
| CVE | CVE-2022-45403 |
| CVE | CVE-2022-45404 |
| CVE | CVE-2022-45405 |
| CVE | CVE-2022-45406 |
| CVE | CVE-2022-45407 |
| CVE | CVE-2022-45408 |
| CVE | CVE-2022-45409 |
| CVE | CVE-2022-45410 |
| CVE | CVE-2022-45411 |
| CVE | CVE-2022-45412 |
| CVE | CVE-2022-45413 |
| CVE | CVE-2022-45415 |
| CVE | CVE-2022-45416 |
| CVE | CVE-2022-45417 |
| CVE | CVE-2022-45418 |
| CVE | CVE-2022-45419 |
| CVE | CVE-2022-45420 |
| CVE | CVE-2022-45421 |
| XREF | USN:5726-1 |
| XREF | IAVA:2022-A-0491-S |

Plugin Information

Published: 2022/11/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_107.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_107.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_107.0+build2-0ubuntu0.20.04.1

168840 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5782-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5782-1 advisory.

It was discovered that Firefox was using an out-of-date libusrstcp library. An attacker could possibly use this library to perform a reentrancy issue on Firefox. (CVE-2022-46871)

Nika Layzell discovered that Firefox was not performing a check on paste received from cross-processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)

Pete Freitag discovered that Firefox did not implement the unsafe-hashes CSP directive. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2022-46873)

Matthias Zoellner discovered that Firefox was not keeping the filename ending intact when using the drag- and-drop event. An attacker could possibly use this

issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)

Hafizh discovered that Firefox was not handling fullscreen notifications when the browser window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-46878,

CVE-2022-46879)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5782-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-46871 |
| CVE | CVE-2022-46872 |
| CVE | CVE-2022-46873 |
| CVE | CVE-2022-46874 |
| CVE | CVE-2022-46877 |
| CVE | CVE-2022-46878 |
| CVE | CVE-2022-46879 |
| XREF | USN:5782-1 |
| XREF | IAVA:2022-A-0517-S |

Plugin Information

Published: 2022/12/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_108.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_108.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_108.0+build2-0ubuntu0.20.04.1

170280 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5816-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5816-1 advisory.

Niklas Baumstark discovered that a compromised web child process of Firefox could disable web security opening restrictions, leading to a new child process being spawned within the file:// context. An attacker could potentially exploit this to obtain sensitive information. (CVE-2023-23597)

Tom Schuster discovered that Firefox was not performing a validation check on GTK drag data. An attacker could potentially exploit this to obtain sensitive information. (CVE-2023-23598)

Vadim discovered that Firefox was not properly sanitizing a curl command output when copying a network request from the developer tools panel. An attacker could potentially exploit this to hide and execute arbitrary commands. (CVE-2023-23599)

Luan Herrera discovered that Firefox was not stopping navigation when dragging a URL from a cross-origin iframe into the same tab. An attacker potentially exploits this to spoof the user. (CVE-2023-23601)

Dave Vandyke discovered that Firefox did not properly implement CSP policy when creating a WebSocket in a WebWorker. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2023-23602)

Dan Veditz discovered that Firefox did not properly implement CSP policy on regular expression when using console.log. An attacker potentially exploits this to exfiltrate data from the browser. (CVE-2023-23603)

Nika Layzell discovered that Firefox was not performing a validation check when parsing a non-system html document via DOMParser::ParseFromSafeString. An attacker potentially exploits this to bypass web security checks. (CVE-2023-23604)

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-23605, CVE-2023-23606)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5816-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-23597 |
| CVE | CVE-2023-23598 |
| CVE | CVE-2023-23599 |
| CVE | CVE-2023-23601 |
| CVE | CVE-2023-23602 |
| CVE | CVE-2023-23603 |
| CVE | CVE-2023-23604 |
| CVE | CVE-2023-23605 |
| CVE | CVE-2023-23606 |
| XREF | USN:5816-1 |
| XREF | IAVA:2023-A-0048-S |

Plugin Information

Published: 2023/01/23, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_109.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_109.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_109.0+build2-0ubuntu0.20.04.1

171637 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5880-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5880-1 advisory.

Christian Holler discovered that Firefox did not properly manage memory when using PKCS 12 Safe Bag attributes. An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes. (CVE-2023-0767)

Johan Carlsson discovered that Firefox did not properly manage child iframe's unredacted URI when using Content-Security-Policy-Report-Only header. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-25728)

Vitor Torres discovered that Firefox did not properly manage permissions of extensions interaction via ExpandedPrincipals. An attacker could potentially exploits this issue to download malicious files or execute arbitrary code. (CVE-2023-25729)

Irvan Kurniawan discovered that Firefox did not properly validate background script invoking requestFullscreen. An attacker could potentially exploit this issue to perform spoofing attacks.
(CVE-2023-25730)

Ronald Crane discovered that Firefox did not properly manage memory when using EncodeInputStream in xpcom.
An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25732)

Samuel Grob discovered that Firefox did not properly manage memory when using wrappers wrapping a scripted proxy. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25735)

Holger Fuhrmann discovered that Firefox did not properly manage memory when using Module load requests.
An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25739)

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25731, CVE-2023-25733, CVE-2023-25736, CVE-2023-25737, CVE-2023-25741, CVE-2023-25742, CVE-2023-25744, CVE-2023-25745)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5880-1>

Solution

Update the affected 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-2023-0767 |
| CVE | CVE-2023-25728 |
| CVE | CVE-2023-25729 |
| CVE | CVE-2023-25730 |
| CVE | CVE-2023-25731 |
| CVE | CVE-2023-25732 |
| CVE | CVE-2023-25733 |
| CVE | CVE-2023-25735 |
| CVE | CVE-2023-25736 |
| CVE | CVE-2023-25737 |
| CVE | CVE-2023-25739 |
| CVE | CVE-2023-25741 |
| CVE | CVE-2023-25742 |
| CVE | CVE-2023-25744 |
| CVE | CVE-2023-25745 |
| XREF | USN:5880-1 |
| XREF | IAVA:2023-A-0081-S |

Plugin Information

Published: 2023/02/20, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_110.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_110.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_110.0+build3-0ubuntu0.20.04.1

172575 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5954-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5954-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25750, CVE-2023-25752, CVE-2023-28162, CVE-2023-28176, CVE-2023-28177)

Lukas Bernhard discovered that Firefox did not properly manage memory when invalidating JIT code while following an iterator. An attacker could potentially exploit this issue to cause a denial of service.

(CVE-2023-25751)

Rob Wu discovered that Firefox did not properly manage the URLs when following a redirect to a publicly accessible web extension file. An attacker could potentially exploit this to obtain sensitive information. (CVE-2023-28160)

Luan Herrera discovered that Firefox did not properly manage cross-origin iframe when dragging a URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-28164)

Khiem Tran discovered that Firefox did not properly manage one-time permissions granted to a document loaded using a file: URL. An attacker could potentially exploit this issue to use granted one-time permissions on the local files came from different sources. (CVE-2023-28161)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5954-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-25750 |
| CVE | CVE-2023-25751 |
| CVE | CVE-2023-25752 |
| CVE | CVE-2023-28160 |
| CVE | CVE-2023-28161 |
| CVE | CVE-2023-28162 |
| CVE | CVE-2023-28164 |
| CVE | CVE-2023-28176 |
| CVE | CVE-2023-28177 |
| XREF | USN:5954-1 |
| XREF | IAVA:2023-A-0132-S |

Plugin Information

Published: 2023/03/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_111.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_111.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_111.0+build2-0ubuntu0.20.04.1

174173 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-6010-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6010-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-29537, CVE-2023-29540, CVE-2023-29543, CVE-2023-29544, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551)

Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)

Lukas Bernhard discovered that Firefox did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service.
(CVE-2023-29535)

Zx from qriousec discovered that Firefox did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service.
(CVE-2023-29536)

Alexis aka zoracon discovered that Firefox did not properly validate the URI received by the WebExtension during a load request. An attacker could potentially exploits this to obtain sensitive information.
(CVE-2023-29538)

Trung Pham discovered that Firefox did not properly validate the filename directive in the Content- Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)

Ameen Basha M K discovered that Firefox did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6010-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-29533 |
| CVE | CVE-2023-29535 |
| CVE | CVE-2023-29536 |
| CVE | CVE-2023-29537 |
| CVE | CVE-2023-29538 |
| CVE | CVE-2023-29539 |
| CVE | CVE-2023-29540 |
| CVE | CVE-2023-29541 |
| CVE | CVE-2023-29543 |
| CVE | CVE-2023-29544 |
| CVE | CVE-2023-29547 |
| CVE | CVE-2023-29548 |
| CVE | CVE-2023-29549 |
| CVE | CVE-2023-29550 |
| CVE | CVE-2023-29551 |
| XREF | USN:6010-1 |
| XREF | IAVA:2023-A-0182-S |

Plugin Information

Published: 2023/04/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_112.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_112.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_112.0+build2-0ubuntu0.20.04.1

175671 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-6074-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6074-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-32216)

Irvan Kurniawan discovered that Firefox did not properly manage memory when using RLBox Expat driver. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)

Anne van Kesteren discovered that Firefox did not properly validate the import() call in service workers. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-32208)

Sam Ezeh discovered that Firefox did not properly handle certain favicon image files. If a user were tricked into opening a malicious favicon file, an attacker could cause a denial of service. (CVE-2023-32209)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6074-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE

CVE-2023-32205

| | |
|------|--------------------|
| CVE | CVE-2023-32206 |
| CVE | CVE-2023-32207 |
| CVE | CVE-2023-32208 |
| CVE | CVE-2023-32209 |
| CVE | CVE-2023-32210 |
| CVE | CVE-2023-32211 |
| CVE | CVE-2023-32212 |
| CVE | CVE-2023-32213 |
| CVE | CVE-2023-32215 |
| CVE | CVE-2023-32216 |
| XREF | USN:6074-1 |
| XREF | IAVA:2023-A-0242-S |

Plugin Information

Published: 2023/05/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_113.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_113.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_113.0+build2-0ubuntu0.20.04.1

165204 - Ubuntu 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-5615-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5615-1 advisory.

It was discovered that SQLite incorrectly handled INTERSEC query processing. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2020-35525)

It was discovered that SQLite incorrectly handled ALTER TABLE for views that have a nested FROM clause.

An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue was only addressed in Ubuntu 20.04 LTS. (CVE-2020-35527)

It was discovered that SQLite incorrectly handled embedded null characters when tokenizing certain unicode strings. This issue could result in incorrect results. This issue only affected Ubuntu 20.04 LTS.

(CVE-2021-20223)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5615-1>

Solution

Update the affected 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 |
| XREF | USN:5615-1 |

Plugin Information

Published: 2022/09/15, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.4

159189 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5345-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5345-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, obtain sensitive information, cause undefined behaviour, spoof the browser UI, or execute arbitrary code. (CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22763, CVE-2022-22764, CVE-2022-26381, CVE-2022-26383, CVE-2022-26384)

It was discovered that extensions of a particular type could auto-update themselves and bypass the prompt that requests permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to bypass security restrictions. (CVE-2022-22754)

It was discovered that dragging and dropping an image into a folder could result in it being marked as executable. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to execute arbitrary code. (CVE-2022-22756)

It was discovered that files downloaded to /tmp were accessible to other users. A local attacker could exploit this to obtain sensitive information. (CVE-2022-26386)

A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature.

(CVE-2022-26387)

An out-of-bounds write by one byte was discovered when processing messages in some circumstances. If a user were tricked into opening a specially crafted message, an attacker could potentially exploit this to cause a denial of service. (CVE-2022-0566)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5345-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.6 (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-2022-0566 |
| CVE | CVE-2022-22754 |
| CVE | CVE-2022-22756 |
| CVE | CVE-2022-22759 |
| CVE | CVE-2022-22760 |
| CVE | CVE-2022-22761 |
| CVE | CVE-2022-22763 |
| CVE | CVE-2022-22764 |
| CVE | CVE-2022-26381 |
| CVE | CVE-2022-26383 |
| CVE | CVE-2022-26384 |
| CVE | CVE-2022-26386 |
| CVE | CVE-2022-26387 |
| XREF | USN:5345-1 |
| XREF | IAVA:2022-A-0103-S |
| XREF | IAVA:2022-A-0079-S |
| XREF | IAVA:2022-A-0088-S |

Plugin Information

Published: 2022/03/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:91.7.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:91.7.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:91.7.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:91.7.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:91.7.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:91.7.0+build2-0ubuntu0.20.04.1

160275 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5393-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5393-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, conduct spoofing attacks, or execute arbitrary code. (CVE-2022-1097, CVE-2022-1196, CVE-2022-28281, CVE-2022-28282, CVE-2022-28285, CVE-2022-28286, CVE-2022-28289)

It was discovered that Thunderbird ignored OpenPGP revocation when importing a revoked key in some circumstances. An attacker could potentially exploit this by tricking the user into trusting the authenticity of a message or tricking them into use a revoked key to send an encrypted message. (CVE-2022-1197)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5393-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1097 |
| CVE | CVE-2022-1196 |
| CVE | CVE-2022-1197 |
| CVE | CVE-2022-28281 |
| CVE | CVE-2022-28282 |
| CVE | CVE-2022-28285 |
| CVE | CVE-2022-28286 |
| CVE | CVE-2022-28289 |
| XREF | USN:5393-1 |
| XREF | IAVA:2022-A-0134-S |

Plugin Information

Published: 2022/04/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:91.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:91.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:91.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:91.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:91.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:91.8.1+build1-0ubuntu0.20.04.1

186445 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : FreeRDP vulnerabilities (USN-6522-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6522-1 advisory.

It was discovered that FreeRDP incorrectly handled drive redirection. If a user were tricked into connection to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2022-41877)

It was discovered that FreeRDP incorrectly handled certain surface updates. A remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-39352, CVE-2023-39356)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6522-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-41877 |
| CVE | CVE-2023-39352 |
| CVE | CVE-2023-39356 |
| XREF | USN:6522-1 |

Plugin Information

Published: 2023/11/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.6
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.6
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.6

183231 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Ghostscript vulnerability (USN-6433-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6433-1 advisory.

It was discovered that Ghostscript incorrectly handled certain PDF documents. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6433-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2023-43115 |
| XREF | USN:6433-1 |
| XREF | IAVB:2023-B-0070-S |

Plugin Information

Published: 2023/10/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `ghostscript_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript_9.50~dfsg-5ubuntu4.11`
- Installed package : `ghostscript-x_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript-x_9.50~dfsg-5ubuntu4.11`
- Installed package : `libgs9_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9_9.50~dfsg-5ubuntu4.11`
- Installed package : `libgs9-common_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9-common_9.50~dfsg-5ubuntu4.11`

187105 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6560-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6560-1 advisory.

Fabian Bumer, Marcus Brinkmann, Jrg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue. (CVE-2023-48795)

Luci Stanescu discovered that OpenSSH incorrectly added destination constraints when smartcard keys were added to ssh-agent, contrary to expectations. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04.

(CVE-2023-28531)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6560-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-28531 |
| CVE | CVE-2023-48795 |
| XREF | IAVA:2023-A-0152-S |
| XREF | USN:6560-1 |
| XREF | IAVA:2023-A-0703 |

Plugin Information

Published: 2023/12/19, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.10
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.10
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.10
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.10

186300 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Perl vulnerabilities (USN-6517-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6517-1 advisory.

It was discovered that Perl incorrectly handled printing certain warning messages. An attacker could possibly use this issue to cause Perl to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-48522)

Nathan Mills discovered that Perl incorrectly handled certain regular expressions. An attacker could use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2023-47038)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6517-1>

Solution

Update the affected 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/Vl: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-2022-48522 |
| CVE | CVE-2023-47038 |
| XREF | USN:6517-1 |

Plugin Information

Published: 2023/11/27, Modified: 2024/09/18

Plugin Output

tcp/0

```
- Installed package : libperl5.30_5.30.0-9build1
- Fixed package : libperl5.30_5.30.0-9ubuntu0.5

- Installed package : perl_5.30.0-9build1
- Fixed package : perl_5.30.0-9ubuntu0.5

- Installed package : perl-base_5.30.0-9build1
- Fixed package : perl-base_5.30.0-9ubuntu0.5

- Installed package : perl-modules-5.30_5.30.0-9build1
- Fixed package : perl-modules-5.30_5.30.0-9ubuntu0.5
```

184190 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6468-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6468-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-5724, CVE-2023-5728, CVE-2023-5730, CVE-2023-5732)

Kelsey Gilbert discovered that Thunderbird did not properly manage certain browser prompts and dialogs due to an insufficient activation-delay. An attacker could potentially exploit this issue to perform clickjacking. (CVE-2023-5721)

Shaheen Fazim discovered that Thunderbird did not properly validate the URLs open by installed WebExtension. An attacker could potentially exploit this issue to obtain sensitive information.

(CVE-2023-5725)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6468-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2023-5721 |
| CVE | CVE-2023-5724 |
| CVE | CVE-2023-5725 |
| CVE | CVE-2023-5728 |
| CVE | CVE-2023-5730 |
| CVE | CVE-2023-5732 |
| XREF | USN:6468-1 |
| XREF | IAVA:2023-A-0585-S |

Plugin Information

Published: 2023/11/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.4.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.4.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.4.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.4.1+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.4.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.4.1+build1-0ubuntu0.20.04.1

186291 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6515-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6515-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-6206, CVE-2023-6212)

It was discovered that Thunderbird did not properly manage memory when images were created on the canvas element. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6204)

It discovered that Thunderbird incorrectly handled certain memory when using a MessagePort. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6205)

It discovered that Thunderbird incorrectly did not properly manage ownership in ReadableByteStreams. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6207)

It discovered that Thunderbird incorrectly did not properly manage copy operations when using Selection API in X11. An attacker could potentially exploit this issue to obtain sensitive information.

(CVE-2023-6208)

Rachmat Abdul Rokhim discovered that Thunderbird incorrectly handled parsing of relative URLs starting with //. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6209)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6515-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|---------------|
| CVE | CVE-2023-6204 |
| CVE | CVE-2023-6205 |
| CVE | CVE-2023-6206 |
| CVE | CVE-2023-6207 |
| CVE | CVE-2023-6208 |
| CVE | CVE-2023-6209 |

CVE
XREF
CVE-2023-6212
USN:6515-1

Plugin Information

Published: 2023/11/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.5.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.5.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.5.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.5.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.5.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.5.0+build1-0ubuntu0.20.04.1

187429 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6563-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6563-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code.(CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6861, CVE-2023-6862, CVE-2023-6863, CVE-2023-6864)

Marcus Brinkmann discovered that Thunderbird did not properly parse a PGP/MIME payload that contains digitally signed text. An attacker could potentially exploit this issue to spoof an email message.

(CVE-2023-50762)

Marcus Brinkmann discovered that Thunderbird did not properly compare the signature creation date with the message date and time when using digitally signed S/MIME email message. An attacker could potentially exploit this issue to spoof date and time of an email message. (CVE-2023-50761)

DoHyun Lee discovered that Thunderbird did not properly manage memory when used on systems with the Mesa VM driver. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2023-6856)

Andrew Osmond discovered that Thunderbird did not properly validate the textures produced by remote decoders. An attacker could potentially exploit this issue to escape the sandbox. (CVE-2023-6860)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6563-1>

Solution

Update the affected 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

7.7 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-6856 |
| CVE | CVE-2023-6857 |
| CVE | CVE-2023-6858 |
| CVE | CVE-2023-6859 |
| CVE | CVE-2023-6860 |
| CVE | CVE-2023-6861 |
| CVE | CVE-2023-6862 |
| CVE | CVE-2023-6863 |
| CVE | CVE-2023-6864 |
| CVE | CVE-2023-50761 |
| CVE | CVE-2023-50762 |
| XREF | USN:6563-1 |
| XREF | IAVA:2023-A-0702-S |

Plugin Information

Published: 2024/01/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.6.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.6.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.6.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.6.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.6.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.6.0+build2-0ubuntu0.20.04.1

189087 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6587-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6587-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs. An attacker could possibly use this issue to cause the X Server to crash, obtain sensitive information, or execute arbitrary code. (CVE-2023-6816)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled reattaching to a different master device. An attacker could use this issue to cause the X Server to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2024-0229)

Olivier Fourdan and Donn Seeley discovered that the X.Org X Server incorrectly labeled GLX PBuffers when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service. (CVE-2024-0408)

Olivier Fourdan discovered that the X.Org X Server incorrectly handled the cursor code when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service.
(CVE-2024-0409)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the XISendDeviceHierarchyEvent API. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21885)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled devices being disabled. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21886)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6587-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-6816 |
| CVE | CVE-2024-0229 |
| CVE | CVE-2024-0408 |
| CVE | CVE-2024-0409 |
| CVE | CVE-2024-21885 |
| CVE | CVE-2024-21886 |
| XREF | USN:6587-1 |

Plugin Information

Published: 2024/01/16, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.14

- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.14

- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.14

- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.14

- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.14
```

182791 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUE vulnerability (USN-6423-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6423-1 advisory.

It was discovered that CUE incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6423-1>

Solution

Update the affected libcue-dev and / or libcue2 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-43641 |
| XREF | USN:6423-1 |

Plugin Information

Published: 2023/10/09, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libcue2_2.2.1-2
- Fixed package : libcue2_2.2.1-2ubuntu0.1

179246 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : GStreamer Base Plugins vulnerabilities (USN-6268-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6268-1 advisory.

It was discovered that GStreamer Base Plugins incorrectly handled certain FLAC image tags. A remote attacker could use this issue to cause GStreamer Base Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37327)

It was discovered that GStreamer Base Plugins incorrectly handled certain subtitles. A remote attacker could use this issue to cause GStreamer Base Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37328)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6268-1>

Solution

Update the affected 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

7.7 (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-2023-37327 |
| CVE | CVE-2023-37328 |
| XREF | USN:6268-1 |

Plugin Information

Published: 2023/08/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-gst-plugins-base-1.0_1.16.2-4
- Fixed package : gir1.2-gst-plugins-base-1.0_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-alsa_1.16.2-4
- Fixed package : gstreamer1.0-alsa_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-gl_1.16.2-4
- Fixed package : gstreamer1.0-gl_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-plugins-base_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-plugins-base-apps_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base-apps_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-x_1.16.2-4
- Fixed package : gstreamer1.0-x_1.16.3-0ubuntu1.2
- Installed package : libgstreamer-gl1.0-0_1.16.2-4
- Fixed package : libgstreamer-gl1.0-0_1.16.3-0ubuntu1.2
- Installed package : libgstreamer-plugins-base1.0-0_1.16.2-4
- Fixed package : libgstreamer-plugins-base1.0-0_1.16.3-0ubuntu1.2

179247 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : GStreamer Good Plugins vulnerability (USN-6269-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6269-1 advisory.

It was discovered that GStreamer Good Plugins incorrectly handled certain FLAC image tags. A remote attacker could use this issue to cause GStreamer Good Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37327)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6269-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2023-37327
XREF-USN:6269-1

Plugin Information

Published: 2023/08/02, Modified: 2024/12/18

Plugin Output

tcp/0

- Installed package : gstreamer1.0-gtk3_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-gtk3_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-plugins-good_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-plugins-good_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-pulseaudio_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-pulseaudio_1.16.3-0ubuntu1.2
- Installed package : libgstreamer-plugins-good1.0-0_1.16.2-1ubuntu2
- Fixed package : libgstreamer-plugins-good1.0-0_1.16.3-0ubuntu1.2

178755 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : OpenSSH vulnerability (USN-6242-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6242-1 advisory.

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 user's system and execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6242-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VCH/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 | USN:6242-1 |
| XREF | IAVA:2023-A-0377-S |

Plugin Information

Published: 2023/07/24, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.8
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.8
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.8
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.8

178210 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6214-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6214-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-37201, CVE-2023-37202, CVE-2023-37207, CVE-2023-37211)

P Umar Farooq discovered that Thunderbird did not properly provide warning when opening Diagcab files. If a user were tricked into opening a malicious Diagcab file, an attacker could execute arbitrary code.

(CVE-2023-37208)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6214-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-34414 |
| CVE | CVE-2023-34416 |
| CVE | CVE-2023-37201 |
| CVE | CVE-2023-37202 |
| CVE | CVE-2023-37207 |
| CVE | CVE-2023-37208 |
| CVE | CVE-2023-37211 |
| XREF | USN:6214-1 |
| XREF | IAVA:2023-A-0284-S |
| XREF | IAVA:2023-A-0331-S |

Plugin Information

Published: 2023/07/12, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.13.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.13.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.13.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.13.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.13.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.13.0+build1-0ubuntu0.20.04.1
```

180468 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6333-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6333-1 advisory.

Junsung Lee discovered that Thunderbird did not properly validate the text direction override unicode character in filenames. An attacker could potentially exploits this issue by spoofing file extension while attaching a file in emails. (CVE-2023-3417)

Max Vlasov discovered that Thunderbird Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same- origin policy. (CVE-2023-4045)

Alexander Guryanov discovered that Thunderbird did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)

Mark Brand discovered that Thunderbird did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4055, CVE-2023-4056)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6333-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2023-3417 |
| CVE | CVE-2023-4045 |
| CVE | CVE-2023-4046 |
| CVE | CVE-2023-4047 |
| CVE | CVE-2023-4048 |
| CVE | CVE-2023-4049 |
| CVE | CVE-2023-4050 |
| CVE | CVE-2023-4055 |
| CVE | CVE-2023-4056 |
| XREF | IAVA:2023-A-0379-S |
| XREF | USN:6333-1 |

Plugin Information

Published: 2023/09/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:102.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.15.0+build1-0ubuntu0.20.04.1

181411 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6368-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6368-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4581, CVE-2023-4584)

It was discovered that Thunderbird did not properly manage memory when handling WebP images. If a user were tricked into opening a malicious WebP image file, an attacker could potentially exploit these to cause a denial of service or execute arbitrary code. (CVE-2023-4863)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6368-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-4573 |
| CVE | CVE-2023-4574 |
| CVE | CVE-2023-4575 |
| CVE | CVE-2023-4581 |
| CVE | CVE-2023-4584 |
| CVE | CVE-2023-4863 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/04 |
| XREF | USN:6368-1 |
| XREF | IAVA:2023-A-0449-S |

Plugin Information

Published: 2023/09/14, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:102.15.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1

- Fixed package : thunderbird-gnome-support_1:102.15.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:102.15.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:102.15.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:102.15.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:102.15.1+build1-0ubuntu0.20.04.1

182432 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6405-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6405-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4057, CVE-2023-4577, CVE-2023-4578, CVE-2023-4583, CVE-2023-4585, CVE-2023-5169, CVE-2023-5171, CVE-2023-5176)

Andrew McCreight discovered that Thunderbird did not properly manage during the worker lifecycle. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-3600)

Harveer Singh discovered that Thunderbird did not store push notifications in private browsing mode in encrypted form. An attacker could potentially exploit this issue to obtain sensitive information.

(CVE-2023-4580)

Clement Lecigne discovered that Thunderbird did not properly manage memory when handling VP8 media stream. An attacker-controlled VP8 media stream could lead to a heap buffer overflow in the content process, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-5217)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6405-1>

Solution

Update the affected 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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|---------------|
| CVE | CVE-2023-3600 |
| CVE | CVE-2023-4057 |
| CVE | CVE-2023-4577 |
| CVE | CVE-2023-4578 |

| | |
|------|---------------------------------|
| CVE | CVE-2023-4580 |
| CVE | CVE-2023-4583 |
| CVE | CVE-2023-4585 |
| CVE | CVE-2023-5169 |
| CVE | CVE-2023-5171 |
| CVE | CVE-2023-5176 |
| CVE | CVE-2023-5217 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/23 |
| XREF | IAVA:2023-A-0379-S |
| XREF | IAVA:2023-A-0449-S |
| XREF | USN:6405-1 |
| XREF | IAVA:2023-A-0507-S |

Plugin Information

Published: 2023/10/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.3.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.3.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.3.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.3.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.3.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.3.1+build1-0ubuntu0.20.04.1

182907 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : curl vulnerabilities (USN-6429-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6429-1 advisory.

Jay Satiro discovered that curl incorrectly handled hostnames when using a SOCKS5 proxy. In environments where curl is configured to use a SOCKS5 proxy, a remote attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-38545)

It was discovered that curl incorrectly handled cookies when an application duplicated certain handles. A local attacker could possibly create a cookie file and inject arbitrary cookies into subsequent connections. (CVE-2023-38546)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6429-1>

Solution

Update the affected 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-2023-38545 |
| CVE | CVE-2023-38546 |
| XREF | USN:6429-1 |
| XREF | CEA-ID:CEA-2023-0052 |
| XREF | IAVA:2023-A-0531-S |

Plugin Information

Published: 2023/10/11, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.20

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.20

182421 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libvpx vulnerabilities (USN-6403-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6403-1 advisory.

It was discovered that libvpx did not properly handle certain malformed media files. If an application using libvpx opened a specially crafted file, a remote attacker could cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6403-1>

Solution

Update the affected 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

8.2 (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-2023-5217 |
| CVE | CVE-2023-44488 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/23 |
| XREF | USN:6403-1 |

Plugin Information

Published: 2023/10/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libvpx6_1.8.2-1build1
- Fixed package : libvpx6_1.8.2-1ubuntu0.2

181426 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6369-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6369-1 advisory.

It was discovered that libwebp incorrectly handled certain malformed images.

If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6369-1>

Solution

Update the affected 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 |
| XREF | USN:6369-1 |

Plugin Information

Published: 2023/09/14, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libwebp6_0.6.1-2
- Fixed package : libwebp6_0.6.1-2ubuntu0.20.04.3

- Installed package : libwebpdemux2_0.6.1-2
- Fixed package : libwebpdemux2_0.6.1-2ubuntu0.20.04.3

- Installed package : libwebpmux3_0.6.1-2
- Fixed package : libwebpdux3_0.6.1-2ubuntu0.20.04.3
```

201972 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6885-1 advisory.

Marc Stern discovered that the Apache HTTP Server incorrectly handled serving WebSocket protocol upgrades over HTTP/2 connections. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2024-36387)

Orange Tsai discovered that the Apache HTTP Server mod_proxy module incorrectly sent certain request URLs with incorrect encodings to backends. A remote attacker could possibly use this issue to bypass authentication. (CVE-2024-38473)

Orange Tsai discovered that the Apache HTTP Server mod_rewrite module incorrectly handled certain substitutions. A remote attacker could possibly use this issue to execute scripts in directories not directly reachable by any URL, or cause a denial of service. Some environments may require using the new UnsafeAllow3F flag to handle unsafe substitutions. (CVE-2024-38474, CVE-2024-38475, CVE-2024-39573)

Orange Tsai discovered that the Apache HTTP Server incorrectly handled certain response headers. A remote attacker could possibly use this issue to obtain sensitive information, execute local scripts, or perform SSRF attacks. (CVE-2024-38476)

Orange Tsai discovered that the Apache HTTP Server mod_proxy module incorrectly handled certain requests.

A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2024-38477)

It was discovered that the Apache HTTP Server incorrectly handled certain handlers configured via AddType.

A remote attacker could possibly use this issue to obtain source code. (CVE-2024-39884)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6885-1>

Solution

Update the affected 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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2024-36387 |
| CVE | CVE-2024-38473 |
| CVE | CVE-2024-38474 |
| CVE | CVE-2024-38475 |
| CVE | CVE-2024-38476 |
| CVE | CVE-2024-38477 |
| CVE | CVE-2024-39573 |
| CVE | CVE-2024-39884 |
| XREF | USN:6885-1 |
| XREF | IAVA:2024-A-0378-S |
| XREF | CISA-KNOWN-EXPLOITED:2025/05/22 |

Plugin Information

Published: 2024/07/08, Modified: 2025/05/02

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.19
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.19
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.19
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.19

200676 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Ghostscript vulnerabilities (USN-6835-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6835-1 advisory.

It was discovered that Ghostscript did not properly restrict eexec seeds to those specified by the Type 1 Font Format standard when SAFER mode is used. An attacker could use this issue to bypass SAFER restrictions and cause unspecified impact. (CVE-2023-52722) This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.10.

Thomas Rinsma discovered that Ghostscript did not prevent changes to uniprint device argument strings after SAFER is activated, resulting in a format-string vulnerability. An attacker could possibly use this to execute arbitrary code. (CVE-2024-29510)

Zdenek Hutyra discovered that Ghostscript did not properly perform path reduction when validating paths.

An attacker could use this to access file locations outside of those allowed by SAFER policy and possibly execute arbitrary code. (CVE-2024-33869)

Zdenek Hutyra discovered that Ghostscript did not properly check arguments when reducing paths. An attacker could use this to access file locations outside of those allowed by SAFER policy.

(CVE-2024-33870)

Zdenek Hutyra discovered that the Driver parameter for Ghostscript's opvp/oprp device allowed specifying the name of an arbitrary dynamic library to load. An attacker could use this to execute arbitrary code. (CVE-2024-33871)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6835-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-52722 |
| CVE | CVE-2024-29510 |
| CVE | CVE-2024-33869 |
| CVE | CVE-2024-33870 |
| CVE | CVE-2024-33871 |
| XREF | IAVB:2023-B-0097-S |
| XREF | USN:6835-1 |
| XREF | IAVB:2024-B-0074-S |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/06/18, Modified: 2024/11/15

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.12
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.12
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.12
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.12

193871 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : FreeRDP vulnerabilities (USN-6749-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6749-1 advisory.

It was discovered that FreeRDP incorrectly handled certain context resets. If a user were tricked into connecting to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-22211)

Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-32039, CVE-2024-32040)

Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could possibly use this issue to cause FreeRDP to crash, resulting in a denial of service. (CVE-2024-32041, CVE-2024-32458, CVE-2024-32460)

Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause FreeRDP clients and servers to crash, resulting in a denial of service. (CVE-2024-32459)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6749-1>

Solution

Update the affected 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:I/C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2024-22211 |
| CVE | CVE-2024-32039 |
| CVE | CVE-2024-32040 |
| CVE | CVE-2024-32041 |
| CVE | CVE-2024-32458 |
| CVE | CVE-2024-32459 |
| CVE | CVE-2024-32460 |
| XREF | USN:6749-1 |
| XREF | IAVA:2024-A-0259 |

Plugin Information

Published: 2024/04/25, Modified: 2025/02/05

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.6.1+dfsg1-0ubuntu0.20.04.1
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.6.1+dfsg1-0ubuntu0.20.04.1
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.6.1+dfsg1-0ubuntu0.20.04.1

193891 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : FreeRDP vulnerabilities (USN-6752-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6752-1 advisory.

It was discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could possibly use this issue to cause FreeRDP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6752-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-32658 |
| CVE | CVE-2024-32659 |
| CVE | CVE-2024-32660 |
| CVE | CVE-2024-32661 |
| XREF | USN:6752-1 |

Plugin Information

Published: 2024/04/25, Modified: 2025/02/05

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.6.1+dfsg1-0ubuntu0.20.04.2
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.6.1+dfsg1-0ubuntu0.20.04.2
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.6.1+dfsg1-0ubuntu0.20.04.2

191486 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6669-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6669-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-0741, CVE-2024-0742, CVE-2024-0747, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0755, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1936)

Cornel Ionice discovered that Thunderbird did not properly manage memory when opening the print preview dialog. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-0746)

Alfred Peters discovered that Thunderbird did not properly manage memory when storing and re-accessing data on a networking channel. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1546)

Johan Carlsson discovered that Thunderbird incorrectly handled Set-Cookie response headers in multipart HTTP responses. An attacker could potentially exploit this issue to inject arbitrary cookie values. (CVE-2024-1551)

Gary Kwong discovered that Thunderbird incorrectly generated codes on 32-bit ARM devices, which could lead to unexpected numeric conversions or undefined behaviour. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-1552)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6669-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2024-0741 |
| CVE | CVE-2024-0742 |
| CVE | CVE-2024-0746 |
| CVE | CVE-2024-0747 |
| CVE | CVE-2024-0749 |
| CVE | CVE-2024-0750 |
| CVE | CVE-2024-0751 |
| CVE | CVE-2024-0753 |
| CVE | CVE-2024-0755 |
| CVE | CVE-2024-1546 |
| CVE | CVE-2024-1547 |
| CVE | CVE-2024-1548 |
| CVE | CVE-2024-1549 |
| CVE | CVE-2024-1550 |
| CVE | CVE-2024-1551 |
| CVE | CVE-2024-1552 |
| CVE | CVE-2024-1553 |
| XREF | USN:6669-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.8.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.8.1+build1-0ubuntu0.20.04.1

197602 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6782-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6782-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4777)

Thomas Rinsma discovered that Thunderbird did not properly handle type check when handling fonts in PDF.js. An attacker could potentially exploit this issue to execute arbitrary javascript code in PDF.js.

(CVE-2024-4367)

Irwan Kurniawan discovered that Thunderbird did not properly handle certain font styles when saving a page to PDF. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-4770)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6782-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-4367 |
| CVE | CVE-2024-4767 |
| CVE | CVE-2024-4768 |
| CVE | CVE-2024-4769 |
| CVE | CVE-2024-4770 |
| CVE | CVE-2024-4777 |
| XREF | USN:6782-1 |
| XREF | IAVA:2024-A-0279-S |

Plugin Information

Published: 2024/05/22, Modified: 2025/01/23

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.11.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1

- Fixed package : thunderbird-gnome-support_1:115.11.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.11.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.11.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.11.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.11.0+build2-0ubuntu0.20.04.1

213188 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Base Plugins vulnerabilities (USN-7175-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7175-1 advisory.

Antonio Morales discovered that GStreamer Base Plugins incorrectly handled certain malformed media files.

An attacker could use these issues to cause GStreamer Base Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7175-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

8.6 (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/Vl: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-2024-47538 |
| CVE | CVE-2024-47541 |
| CVE | CVE-2024-47542 |
| CVE | CVE-2024-47600 |
| CVE | CVE-2024-47607 |
| CVE | CVE-2024-47615 |
| CVE | CVE-2024-47835 |
| XREF | USN:7175-1 |
| XREF | IAVA:2024-A-0832-S |

Plugin Information

Published: 2024/12/18, Modified: 2025/05/05

Plugin Output

tcp/0

- Installed package : gir1.2-gst-plugins-base-1.0_1.16.2-4
- Fixed package : gir1.2-gst-plugins-base-1.0_1.16.3-0ubuntu1.4
- Installed package : gstreamer1.0-alsa_1.16.2-4
- Fixed package : gstreamer1.0-alsa_1.16.3-0ubuntu1.4
- Installed package : gstreamer1.0-gl_1.16.2-4
- Fixed package : gstreamer1.0-gl_1.16.3-0ubuntu1.4
- Installed package : gstreamer1.0-plugins-base_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base_1.16.3-0ubuntu1.4
- Installed package : gstreamer1.0-plugins-base-apps_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base-apps_1.16.3-0ubuntu1.4
- Installed package : gstreamer1.0-x_1.16.2-4
- Fixed package : gstreamer1.0-x_1.16.3-0ubuntu1.4
- Installed package : libgstreamer-glib1.0-0_1.16.2-4
- Fixed package : libgstreamer-glib1.0-0_1.16.3-0ubuntu1.4
- Installed package : libgstreamer-plugins-base1.0-0_1.16.2-4
- Fixed package : libgstreamer-plugins-base1.0-0_1.16.3-0ubuntu1.4

213187 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Good Plugins vulnerabilities (USN-7176-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7176-1 advisory.

Antonio Morales discovered that GStreamer Good Plugins incorrectly handled certain malformed media files.

An attacker could use these issues to cause GStreamer Good Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7176-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

8.6 (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/V/C:H/V/I: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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-47537 |
| CVE | CVE-2024-47539 |
| CVE | CVE-2024-47540 |
| CVE | CVE-2024-47543 |
| CVE | CVE-2024-47544 |
| CVE | CVE-2024-47545 |
| CVE | CVE-2024-47546 |
| CVE | CVE-2024-47596 |
| CVE | CVE-2024-47597 |
| CVE | CVE-2024-47598 |
| CVE | CVE-2024-47599 |
| CVE | CVE-2024-47601 |
| CVE | CVE-2024-47602 |
| CVE | CVE-2024-47603 |
| CVE | CVE-2024-47606 |
| CVE | CVE-2024-47613 |
| CVE | CVE-2024-47774 |
| CVE | CVE-2024-47775 |
| CVE | CVE-2024-47776 |
| CVE | CVE-2024-47777 |
| CVE | CVE-2024-47778 |
| CVE | CVE-2024-47834 |
| XREF | USN:7176-1 |
| XREF | IAVA:2024-A-0832-S |

Plugin Information

Published: 2024/12/18, Modified: 2025/05/05

Plugin Output

tcp/0

```
- Installed package : gstreamer1.0-gtk3_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-gtk3_1.16.3-0ubuntu1.3

- Installed package : gstreamer1.0-plugins-good_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-plugins-good_1.16.3-0ubuntu1.3

- Installed package : gstreamer1.0-pulseaudio_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-pulseaudio_1.16.3-0ubuntu1.3

- Installed package : libgstreamer-plugins-good1.0-0_1.16.2-1ubuntu2
- Fixed package : libgstreamer-plugins-good1.0-0_1.16.3-0ubuntu1.3
```

213189 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer vulnerability (USN-7174-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7174-1 advisory.

Antonio Morales discovered that GStreamer incorrectly handled allocating memory for certain buffers. An attacker could use this issue to cause GStreamer to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7174-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

8.6 (CVSS:4.0/AV:L/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

8.5 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-47606 |
| XREF | USN:7174-1 |
| XREF | IAVA:2024-A-0832-S |

Plugin Information

Published: 2024/12/18, Modified: 2025/05/05

Plugin Output

tcp/0

- Installed package : gir1.2-gstreamer-1.0_1.16.2-2
- Fixed package : gir1.2-gstreamer-1.0_1.16.3-0ubuntu1.2
- Installed package : gstreamer1.0-tools_1.16.2-2
- Fixed package : gstreamer1.0-tools_1.16.3-0ubuntu1.2
- Installed package : libgstreamer1.0-0_1.16.2-2
- Fixed package : libgstreamer1.0-0_1.16.3-0ubuntu1.2

205548 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : BusyBox vulnerabilities (USN-6961-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6961-1 advisory.

It was discovered that BusyBox did not properly validate user input when performing certain arithmetic operations. If a user or automated system were tricked into processing a specially crafted file, an attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2022-48174)

It was discovered that BusyBox incorrectly managed memory when evaluating certain awk expressions. An attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. This issue only affected Ubuntu 24.04 LTS. (CVE-2023-42363, CVE-2023-42364, CVE-2023-42365)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6961-1>

Solution

Update the affected 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-2022-48174 |
| CVE | CVE-2023-42363 |
| CVE | CVE-2023-42364 |
| CVE | CVE-2023-42365 |
| XREF | USN:6961-1 |

Plugin Information

Published: 2024/08/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : busybox-initramfs_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-initramfs_1:1.30.1-4ubuntu6.5

- Installed package : busybox-static_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-static_1:1.30.1-4ubuntu6.5

202378 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Ghostscript vulnerabilities (USN-6897-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6897-1 advisory.

It was discovered that Ghostscript incorrectly handled certain long PDF filter names. An attacker could possibly use this issue to cause Ghostscript to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-29506)

It was discovered that Ghostscript incorrectly handled certain API parameters. An attacker could possibly use this issue to cause Ghostscript to crash, resulting in a denial of service. This issue only affected Ubuntu 24.04 LTS. (CVE-2024-29507)

It was discovered that Ghostscript incorrectly handled certain BaseFont names. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2024-29508)

It was discovered that Ghostscript incorrectly handled certain PDF passwords that contained NULL bytes. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-29509)

It was discovered that Ghostscript incorrectly handled certain file paths when doing OCR. An attacker could use this issue to read arbitrary files and write error messages to arbitrary files. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-29511)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6897-1>

Solution

Update the affected 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

7.7 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-29506 |
| CVE | CVE-2024-29507 |
| CVE | CVE-2024-29508 |
| CVE | CVE-2024-29509 |
| CVE | CVE-2024-29511 |
| XREF | USN:6897-1 |
| XREF | IAVB:2024-B-0074-S |

Plugin Information

Published: 2024/07/15, Modified: 2024/11/15

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.13
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.13
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.13
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.13

186720 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6544-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6544-1 advisory.

It was discovered that GNU binutils incorrectly handled certain COFF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS.

(CVE-2022-38533)

It was discovered that GNU binutils was not properly performing bounds checks in several functions, which could lead to a buffer overflow. An attacker could possibly use this issue to cause a denial of service, expose sensitive information or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

(CVE-2022-4285, CVE-2020-19726, CVE-2021-46174)

It was discovered that GNU binutils contained a reachable assertion, which could lead to an intentional assertion failure when processing certain crafted DWARF files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS

and Ubuntu 22.04 LTS. (CVE-2022-35205)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6544-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-19726 |
| CVE | CVE-2021-46174 |
| CVE | CVE-2022-4285 |
| CVE | CVE-2022-35205 |
| CVE | CVE-2022-38533 |
| XREF | USN:6544-1 |

Plugin Information

Published: 2023/12/11, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.7

- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.7

- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.7

- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.7

- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.7

- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.7
```

170562 - Ubuntu 20.04 LTS / 22.04 LTS : Samba vulnerabilities (USN-5822-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5822-1 advisory.

It was discovered that Samba incorrectly handled the bad password count logic. A remote attacker could possibly use this issue to bypass bad passwords lockouts.

This issue was only addressed in Ubuntu 22.10.
(CVE-2021-20251)

Evgeny Legerov discovered that Samba incorrectly handled buffers in certain GSSAPI routines of Heimdal. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service.
(CVE-2022-3437)

Tom Tervoort discovered that Samba incorrectly used weak rc4-hmac Kerberos keys. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-37966, CVE-2022-37967)

It was discovered that Samba supported weak RC4/HMAC-MD5 in NetLogon Secure Channel. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-38023)

Greg Hudson discovered that Samba incorrectly handled PAC parsing. On 32-bit systems, a remote attacker could use this issue to escalate privileges, or possibly execute arbitrary code. (CVE-2022-42898)

Joseph Sutton discovered that Samba could be forced to issue rc4-hmac encrypted Kerberos tickets. A remote attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-45141)

WARNING: The fixes included in these updates introduce several important behavior changes which may cause compatibility problems interacting with systems still expecting the former behavior. Please see the following upstream advisories for more information:

<https://www.samba.org/samba/security/CVE-2022-37966.html> <https://www.samba.org/samba/security/CVE-2022-37967.html>
<https://www.samba.org/samba/security/CVE-2022-38023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5822-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-20251 |
| CVE | CVE-2022-3437 |
| CVE | CVE-2022-37966 |
| CVE | CVE-2022-37967 |
| CVE | CVE-2022-38023 |
| CVE | CVE-2022-42898 |
| CVE | CVE-2022-45141 |
| XREF | USN:5822-1 |
| XREF | IAVA:2022-A-0447-S |
| XREF | IAVA:2022-A-0495-S |
| XREF | IAVA:2023-A-0004-S |

Plugin Information

Published: 2023/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsmbclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmbclient_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.17~dfsg-0ubuntu1.20.04.4

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.17~dfsg-0ubuntu1.20.04.4
```

202766 - Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-6903-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6903-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-6600, CVE-2024-6601, CVE-2024-6604)

Ronald Crane discovered that Thunderbird did not properly manage certain memory operations in the NSS. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-6602)

Irvan Kurniawan discovered that Thunderbird did not properly manage memory during thread creation. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code.

(CVE-2024-6603)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6903-1>

Solution

Update the affected 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:I;I/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2024-6600 |
| CVE | CVE-2024-6601 |
| CVE | CVE-2024-6602 |
| CVE | CVE-2024-6603 |
| CVE | CVE-2024-6604 |
| XREF | USN:6903-1 |

Plugin Information

Published: 2024/07/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.13.0+build5-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.13.0+build5-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.13.0+build5-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.13.0+build5-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.13.0+build5-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.13.0+build5-0ubuntu0.20.04.1

206776 - Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-6995-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6995-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-7521, CVE-2024-7526, CVE-2024-7527, CVE-2024-7529, CVE-2024-8382)

It was discovered that Thunderbird did not properly manage certain memory operations when processing graphics shared memory. An attacker could potentially exploit this issue to escape the sandbox.

(CVE-2024-7519)

Irvan Kurniawan discovered that Thunderbird did not properly check an attribute value in the editor component, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-7522)

Rob Wu discovered that Thunderbird did not properly check permissions when creating a StreamFilter. An attacker could possibly use this issue to modify response body of requests on any site using a web extension. (CVE-2024-7525)

Nils Bars discovered that Thunderbird contained a type confusion vulnerability when performing certain property name lookups. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-8381)

It was discovered that Thunderbird did not properly manage memory during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code.

(CVE-2024-8384)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6995-1>

Solution

Update the affected 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-2024-7519 |
| CVE | CVE-2024-7521 |
| CVE | CVE-2024-7522 |
| CVE | CVE-2024-7525 |
| CVE | CVE-2024-7526 |
| CVE | CVE-2024-7527 |
| CVE | CVE-2024-7529 |
| CVE | CVE-2024-8381 |
| CVE | CVE-2024-8382 |
| CVE | CVE-2024-8384 |
| XREF | IAVA:2024-A-0465-S |
| XREF | USN:6995-1 |
| XREF | IAVA:2024-A-0550-S |

Plugin Information

Published: 2024/09/09, Modified: 2025/02/03

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.15.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.15.0+build1-0ubuntu0.20.04.1

208938 - Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerability (USN-7066-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7066-1 advisory.

Damien Schaeffer discovered that Thunderbird did not properly manage certain memory operations when processing content in the Animation timelines. An attacker could potentially exploit this issue to achieve arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7066-1>

Solution

Update the affected 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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2024-9680 |
| XREF | USN:7066-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/11/05 |

Plugin Information

Published: 2024/10/14, Modified: 2024/10/17

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.16.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.16.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.16.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.16.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.16.0+build2-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.16.0+build2-0ubuntu0.20.04.1

161750 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5457-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5457-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5457-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-26700 |
| CVE | CVE-2022-26709 |
| CVE | CVE-2022-26716 |
| CVE | CVE-2022-26717 |
| CVE | CVE-2022-26719 |
| XREF | USN:5457-1 |

Plugin Information

Published: 2022/06/01, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.3-0ubuntu0.20.04.1

- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.3-0ubuntu0.20.04.1

- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.3-0ubuntu0.20.04.1

- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.3-0ubuntu0.20.04.1
```

163270 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5522-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5522-1 advisory.

Several security issues were discovered in WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5522-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-22677 |
| CVE | CVE-2022-26710 |
| XREF | USN:5522-1 |

Plugin Information

Published: 2022/07/18, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1`
- Fixed package : `gir1.2-javascriptcoregtk-4.0_2.36.4-0ubuntu0.20.04.1`
- Installed package : `gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1`
- Fixed package : `gir1.2-webkit2-4.0_2.36.4-0ubuntu0.20.04.1`
- Installed package : `libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1`
- Fixed package : `libjavascriptcoregtk-4.0-18_2.36.4-0ubuntu0.20.04.1`
- Installed package : `libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1`
- Fixed package : `libwebkit2gtk-4.0-37_2.36.4-0ubuntu0.20.04.1`

164124 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5568-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5568-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5568-1>

Solution

Update the affected 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

8.2 (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-2022-2294 |
| CVE | CVE-2022-32792 |
| CVE | CVE-2022-32816 |
| XREF | USN:5568-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/09/15 |

Plugin Information

Published: 2022/08/15, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.6-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.6-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.6-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.6-0ubuntu0.20.04.1

165466 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5642-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5642-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5642-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-32886 |
| XREF | USN:5642-1 |

Plugin Information

Published: 2022/09/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.8-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.8-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.8-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.8-0ubuntu0.20.04.1

167874 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5730-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5730-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5730-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-32888 |
| CVE | CVE-2022-32923 |
| CVE | CVE-2022-42799 |
| CVE | CVE-2022-42823 |
| CVE | CVE-2022-42824 |
| XREF | USN:5730-1 |

Plugin Information

Published: 2022/11/18, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.38.2-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.38.2-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.38.2-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.38.2-0ubuntu0.20.04.1

169734 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5797-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5797-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5797-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2022-42852 |
| CVE | CVE-2022-42856 |
| CVE | CVE-2022-42867 |

| | |
|------|---------------------------------|
| CVE | CVE-2022-46692 |
| CVE | CVE-2022-46698 |
| CVE | CVE-2022-46699 |
| CVE | CVE-2022-46700 |
| XREF | USN:5797-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/01/04 |

Plugin Information

Published: 2023/01/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.38.3-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.38.3-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.38.3-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.38.3-0ubuntu0.20.04.1

171388 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5867-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5867-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5867-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-42826 |
| CVE | CVE-2023-23517 |
| CVE | CVE-2023-23518 |
| XREF | USN:5867-1 |

Plugin Information

Published: 2023/02/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.38.4-0ubuntu0.20.04.2
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.38.4-0ubuntu0.20.04.2
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.38.4-0ubuntu0.20.04.2
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.38.4-0ubuntu0.20.04.2

171943 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5893-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5893-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5893-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-23529 |
| XREF | USN:5893-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/03/07 |

Plugin Information

Published: 2023/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.38.5-0ubuntu0.20.04.1

- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.38.5-0ubuntu0.20.04.1

- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.38.5-0ubuntu0.20.04.1

- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.38.5-0ubuntu0.20.04.1
```

165082 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerability (USN-5611-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5611-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5611-1>

Solution

Update the affected 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

8.2 (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-2022-32893 |
| XREF | USN:5611-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/09/08 |

Plugin Information

Published: 2022/09/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.7-0ubuntu0.20.04.1

- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.7-0ubuntu0.20.04.1

- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.7-0ubuntu0.20.04.1
```

- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.7-0ubuntu0.20.04.1

166179 - Ubuntu 20.04 LTS / 22.04 LTS : zlib vulnerability (USN-5570-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5570-2 advisory.

USN-5570-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 22.04 LTS and Ubuntu 20.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5570-2>

Solution

Update the affected 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 |
| XREF | USN:5570-2 |

Plugin Information

Published: 2022/10/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : zlib1g_1:1.2.11.dfsg-2ubuntu1
- Fixed package : zlib1g_1:1.2.11.dfsg-2ubuntu1.5

176886 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6143-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6143-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-34417)

Jun Kokatsu discovered that Firefox did not properly validate site-isolated process for a document loaded from a data: URL that was the result of a redirect, leading to an open redirect attack. An attacker could possibly use this issue to perform phishing attacks. (CVE-2023-34415)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6143-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-34414 |
| CVE | CVE-2023-34415 |
| CVE | CVE-2023-34416 |
| CVE | CVE-2023-34417 |
| XREF | USN:6143-1 |
| XREF | IAVA:2023-A-0277-S |

Plugin Information

Published: 2023/06/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_114.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_114.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_114.0+build3-0ubuntu0.20.04.1

177998 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6201-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6201-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to

cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-37201, CVE-2023-37202, CVE-2023-37205, CVE-2023-37207, CVE-2023-37209, CVE-2023-37210, CVE-2023-37211, CVE-2023-37212)

Martin Hostettler discovered that Firefox did not properly block storage of all cookies when configured.

An attacker could potentially exploits this issue to store tracking data without permission in localstorage. (CVE-2023-3482)

Paul Nickerson discovered that Firefox did have insufficient validation in the Drag and Drop API. If a user were tricked into creating a shortcut to local system files, an attacker could execute arbitrary code. (CVE-2023-37203)

Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using an option element having an expensive computational function. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-37204)

Ameen Basha M K discovered that Firefox did not properly validate symlinks in the FileSystem API. If a user were tricked into uploading a symlinked file to a malicious website, an attacker could obtain sensitive information. (CVE-2023-37206)

Puf discovered that Firefox did not properly provide warning when opening Diagcab files. If a user were tricked into opening a malicious Diagcab file, an attacker could execute arbitrary code. (CVE-2023-37208)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6201-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-3482 |
| CVE | CVE-2023-37201 |
| CVE | CVE-2023-37202 |
| CVE | CVE-2023-37203 |
| CVE | CVE-2023-37204 |
| CVE | CVE-2023-37205 |
| CVE | CVE-2023-37206 |
| CVE | CVE-2023-37207 |
| CVE | CVE-2023-37208 |
| CVE | CVE-2023-37209 |
| CVE | CVE-2023-37210 |
| CVE | CVE-2023-37211 |
| CVE | CVE-2023-37212 |
| XREF | USN:6201-1 |
| XREF | IAVA:2023-A-0328-S |

Plugin Information

Published: 2023/07/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_115.0+build2-0ubuntu0.20.04.3

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_115.0+build2-0ubuntu0.20.04.3

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_115.0+build2-0ubuntu0.20.04.3
```

179203 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6267-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6267-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4051, CVE-2023-4053, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4058)

Max Vlasov discovered that Firefox Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2023-4045)

Alexander Guryanov discovered that Firefox did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)

Mark Brand discovered that Firefox did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6267-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|---------------|
| CVE | CVE-2023-4045 |
| CVE | CVE-2023-4046 |
| CVE | CVE-2023-4047 |
| CVE | CVE-2023-4048 |
| CVE | CVE-2023-4049 |
| CVE | CVE-2023-4050 |
| CVE | CVE-2023-4051 |

| | |
|------|--------------------|
| CVE | CVE-2023-4053 |
| CVE | CVE-2023-4055 |
| CVE | CVE-2023-4056 |
| CVE | CVE-2023-4057 |
| CVE | CVE-2023-4058 |
| XREF | USN:6267-1 |
| XREF | IAVA:2023-A-0388-S |

Plugin Information

Published: 2023/08/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_116.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_116.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_116.0+build2-0ubuntu0.20.04.2

180274 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6320-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6320-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4578, CVE-2023-4581, CVE-2023-4583, CVE-2023-4584, CVE-2023-4585)

Lukas Bernhard discovered that Firefox did not properly manage memory when the UpdateRegExpStatics attempted to access initialStringHeap. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4577)

Malte Jrgens discovered that Firefox did not properly handle search queries if the search query itself was a well formed URL. An attacker could potentially exploit this issue to perform spoofing attacks.

(CVE-2023-4579)

Harveer Singh discovered that Firefox did not properly handle push notifications stored on disk in private browsing mode. An attacker could potentially exploits this issue to access sensitive information.

(CVE-2023-4580)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6320-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-4573 |
| CVE | CVE-2023-4574 |
| CVE | CVE-2023-4575 |
| CVE | CVE-2023-4577 |
| CVE | CVE-2023-4578 |
| CVE | CVE-2023-4579 |
| CVE | CVE-2023-4580 |
| CVE | CVE-2023-4581 |
| CVE | CVE-2023-4583 |
| CVE | CVE-2023-4584 |
| CVE | CVE-2023-4585 |
| XREF | USN:6320-1 |
| XREF | IAVA:2023-A-0449-S |

Plugin Information

Published: 2023/08/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_117.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_117.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_117.0+build2-0ubuntu0.20.04.1

182431 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6404-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6404-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172, CVE-2023-5175, CVE-2023-5176)

Ronald Crane discovered that Firefox did not properly manage memory when non-HTTPS Alternate Services (network.http.altsvc.oe) is enabled. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5173)

Clment Lecigne discovered that Firefox did not properly manage memory when handling VP8 media stream. An attacker-controlled VP8 media stream could lead to a heap buffer overflow in the content process, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-5217)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6404-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-5169 |
| CVE | CVE-2023-5170 |
| CVE | CVE-2023-5171 |
| CVE | CVE-2023-5172 |
| CVE | CVE-2023-5173 |
| CVE | CVE-2023-5175 |
| CVE | CVE-2023-5176 |
| CVE | CVE-2023-5217 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/23 |
| XREF | USN:6404-1 |
| XREF | IAVA:2023-A-0507-S |
| XREF | IAVA:2023-A-0522-S |

Plugin Information

Published: 2023/10/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_118.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_118.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_118.0.1+build1-0ubuntu0.20.04.1

184009 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6456-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6456-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5722, CVE-2023-5724, CVE-2023-5728, CVE-2023-5729, CVE-2023-5730, CVE-2023-5731)

Kelsey Gilbert discovered that Firefox did not properly manage certain browser prompts and dialogs due to an insufficient activation-delay. An attacker could potentially exploit this issue to perform clickjacking. (CVE-2023-5721)

Daniel Veditz discovered that Firefox did not properly validate a cookie containing invalid characters. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5723)

Shaheen Fazim discovered that Firefox did not properly validate the URLs open by installed WebExtension. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-5725)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6456-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-5721 |
| CVE | CVE-2023-5722 |
| CVE | CVE-2023-5723 |
| CVE | CVE-2023-5724 |
| CVE | CVE-2023-5725 |
| CVE | CVE-2023-5728 |
| CVE | CVE-2023-5729 |
| CVE | CVE-2023-5730 |
| CVE | CVE-2023-5731 |
| XREF | USN:6456-1 |
| XREF | IAVA:2023-A-0585-S |

Plugin Information

Published: 2023/10/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_119.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_119.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_119.0+build2-0ubuntu0.20.04.1

186208 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6509-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6509-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-6206, CVE-2023-6210, CVE-2023-6211, CVE-2023-6212, CVE-2023-6213)

It was discovered that Firefox did not properly manage memory when images were created on the canvas element. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6204)

It was discovered that Firefox incorrectly handled certain memory when using a MessagePort. An attacker could potentially exploit this issue to cause a denial of

service. (CVE-2023-6205)

It discovered that Firefox incorrectly did not properly manage ownership in ReadableByteStreams. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6207)

It discovered that Firefox incorrectly did not properly manage copy operations when using Selection API in X11. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6208)

Rachmat Abdul Rokhim discovered that Firefox incorrectly handled parsing of relative URLs starting with ///. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6209)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6509-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2023-6204 |
| CVE | CVE-2023-6205 |
| CVE | CVE-2023-6206 |
| CVE | CVE-2023-6207 |
| CVE | CVE-2023-6208 |
| CVE | CVE-2023-6209 |
| CVE | CVE-2023-6210 |
| CVE | CVE-2023-6211 |
| CVE | CVE-2023-6212 |
| CVE | CVE-2023-6213 |
| XREF | USN:6509-1 |
| XREF | IAVA:2023-A-0654-S |

Plugin Information

Published: 2023/11/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_120.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_120.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_120.0+build2-0ubuntu0.20.04.1

187406 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6562-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6562-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code.(CVE-2023-6865, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6866, CVE-2023-6867, CVE-2023-6861, CVE-2023-6869, CVE-2023-6871, CVE-2023-6872, CVE-2023-6863, CVE-2023-6864, CVE-2023-6873)

DoHyun Lee discovered that Firefox did not properly manage memory when used on systems with the Mesa VM driver. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2023-6856)

George Pantela and Hubert Kario discovered that Firefox using multiple NSS NIST curves which were susceptible to a side-channel attack known as Minerva. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6135)

Andrew Osmond discovered that Firefox did not properly validate the textures produced by remote decoders.

An attacker could potentially exploit this issue to escape the sandbox. (CVE-2023-6860)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6562-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-6135 |
| CVE | CVE-2023-6856 |
| CVE | CVE-2023-6857 |
| CVE | CVE-2023-6858 |
| CVE | CVE-2023-6859 |
| CVE | CVE-2023-6860 |
| CVE | CVE-2023-6861 |
| CVE | CVE-2023-6863 |
| CVE | CVE-2023-6864 |
| CVE | CVE-2023-6865 |
| CVE | CVE-2023-6866 |
| CVE | CVE-2023-6867 |
| CVE | CVE-2023-6869 |
| CVE | CVE-2023-6871 |
| CVE | CVE-2023-6872 |
| CVE | CVE-2023-6873 |
| XREF | USN:6562-1 |
| XREF | IAVA:2023-A-0702-S |

Plugin Information

Published: 2024/01/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_121.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_121.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_121.0+build1-0ubuntu0.20.04.1

189735 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6610-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6610-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-0741, CVE-2024-0742, CVE-2024-0743, CVE-2024-0744, CVE-2024-0745, CVE-2024-0747, CVE-2024-0748, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0754, CVE-2024-0755)

Cornel Ionce discovered that Firefox did not properly manage memory when opening the print preview dialog. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-0746)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6610-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|-------------------------------|
| CVE | CVE-2024-0741 |
| CVE | CVE-2024-0742 |
| CVE | CVE-2024-0743 |
| CVE | CVE-2024-0744 |
| CVE | CVE-2024-0745 |
| CVE | CVE-2024-0746 |
| CVE | CVE-2024-0747 |

| | |
|------|----------------------|
| CVE | CVE-2024-0748 |
| CVE | CVE-2024-0749 |
| CVE | CVE-2024-0750 |
| CVE | CVE-2024-0751 |
| CVE | CVE-2024-0753 |
| CVE | CVE-2024-0754 |
| CVE | CVE-2024-0755 |
| XREF | USN:6610-1 |
| XREF | IAVA:2024-A-0053-S |
| XREF | IAVA:2024-A-0174-S |

Plugin Information

Published: 2024/01/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_122.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_122.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_122.0+build2-0ubuntu0.20.04.1

192303 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6703-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6703-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-2609, CVE-2024-2611, CVE-2024-2614, CVE-2024-2615)

Hubert Kario discovered that Firefox had a timing side-channel when

performing RSA decryption. A remote attacker could possibly use this

issue to recover sensitive information. (CVE-2023-5388)

It was discovered that Firefox did not properly handle WASM register values in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2606)

Gary Kwong discovered that Firefox incorrectly updated return registers for JIT code on Armv7-A systems.

An attacker could potentially exploit

this issue to execute arbitrary code. (CVE-2024-2607)

Ronald Crane discovered that Firefox did not properly manage memory during character encoding. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2608)

Georg Felber and Marco Squarcina discovered that Firefox incorrectly

handled html and body tags. An attacker who was able to inject markup into

a page otherwise protected by a Content Security Policy may have been able

to obtain sensitive information. (CVE-2024-2610)

Ronald Crane discovered a use-after-free in Firefox when handling code in SafeRefPtr. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-2612)

Max Inden discovered that Firefox incorrectly handled QUIC ACK frame

decoding. An attacker could potentially exploit this issue to cause a

denial of service. (CVE-2024-2613)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6703-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-5388 |
| CVE | CVE-2024-2606 |
| CVE | CVE-2024-2607 |
| CVE | CVE-2024-2608 |
| CVE | CVE-2024-2609 |
| CVE | CVE-2024-2610 |
| CVE | CVE-2024-2611 |
| CVE | CVE-2024-2612 |
| CVE | CVE-2024-2613 |
| CVE | CVE-2024-2614 |
| CVE | CVE-2024-2615 |
| XREF | USN:6703-1 |
| XREF | IAVA:2024-A-0174-S |
| XREF | IAVA:2024-A-0245-S |

Plugin Information

Published: 2024/03/20, Modified: 2025/04/02

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_124.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_124.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_124.0+build1-0ubuntu0.20.04.1

192523 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6710-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6710-1 advisory.

Manfred Paul discovered that Firefox did not properly perform bounds checking during range analysis, leading to an out-of-bounds write vulnerability. A attacker could use this to cause a denial of service,

or execute arbitrary code. (CVE-2024-29943)

Manfred Paul discovered that Firefox incorrectly handled MessageManager

listeners under certain circumstances. An attacker who was able to inject

an event handler into a privileged object may have been able to execute

arbitrary code. (CVE-2024-29944)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6710-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-29943 |
| CVE | CVE-2024-29944 |
| XREF | USN:6710-1 |
| XREF | IAVA:2024-A-0174-S |

Plugin Information

Published: 2024/03/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_124.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_124.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_124.0.1+build1-0ubuntu0.20.04.1

197537 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6779-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6779-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4771, CVE-2024-4772, CVE-2024-4773, CVE-2024-4774, CVE-2024-4775, CVE-2024-4776, CVE-2024-4777, CVE-2024-4778)

Jan-Ivar Bruaroey discovered that Firefox did not properly manage memory when audio input connected with multiple consumers. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-4764)

Thomas Rinsma discovered that Firefox did not properly handle type check when handling fonts in PDF.js. An attacker could potentially exploit this issue to execute arbitrary javascript code in PDF.js.

(CVE-2024-4367)

Irvan Kurniawan discovered that Firefox did not properly handle certain font styles when saving a page to PDF. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-4770)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6779-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-4367 |
| CVE | CVE-2024-4764 |
| CVE | CVE-2024-4767 |
| CVE | CVE-2024-4768 |
| CVE | CVE-2024-4769 |
| CVE | CVE-2024-4770 |
| CVE | CVE-2024-4771 |
| CVE | CVE-2024-4772 |
| CVE | CVE-2024-4773 |
| CVE | CVE-2024-4774 |
| CVE | CVE-2024-4775 |
| CVE | CVE-2024-4776 |
| CVE | CVE-2024-4777 |
| CVE | CVE-2024-4778 |
| XREF | USN:6779-1 |
| XREF | IAVA:2024-A-0279-S |

Plugin Information

Published: 2024/05/21, Modified: 2025/03/19

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_126.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_126.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_126.0+build2-0ubuntu0.20.04.1
```

201338 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6862-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6862-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-5689, CVE-2024-5690, CVE-2024-5691, CVE-2024-5693, CVE-2024-5697, CVE-2024-5698, CVE-2024-5699, CVE-2024-5700, CVE-2024-5701)

Lukas Bernhard discovered that Firefox did not properly manage memory during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or

execute arbitrary code. (CVE-2024-5688)

Lukas Bernhard discovered that Firefox did not properly manage memory in the JavaScript engine. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2024-5694)

Irvan Kurniawan discovered that Firefox did not properly handle certain allocations in the probabilistic heap checker. An attacker could potentially exploit this issue to cause a denial of service.

(CVE-2024-5695)

Irvan Kurniawan discovered that Firefox did not properly handle certain text fragments in input tags. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-5696)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6862-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-5688 |
| CVE | CVE-2024-5689 |
| CVE | CVE-2024-5690 |
| CVE | CVE-2024-5691 |
| CVE | CVE-2024-5693 |
| CVE | CVE-2024-5694 |
| CVE | CVE-2024-5695 |
| CVE | CVE-2024-5696 |
| CVE | CVE-2024-5697 |
| CVE | CVE-2024-5698 |
| CVE | CVE-2024-5699 |
| CVE | CVE-2024-5700 |
| CVE | CVE-2024-5701 |
| XREF | USN:6862-1 |
| XREF | IAVA:2024-A-0335-S |

Plugin Information

Published: 2024/07/03, Modified: 2025/04/07

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_127.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_127.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_127.0.2+build1-0ubuntu0.20.04.1

202049 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6890-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6890-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-6601, CVE-2024-6604, CVE-2024-6607, CVE-2024-6608, CVE-2024-6610, CVE-2024-6611, CVE-2024-6612, CVE-2024-6613, CVE-2024-6614, CVE-2024-6615)

It was discovered that Firefox did not properly manage certain memory operations in the NSS. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code.

(CVE-2024-6602, CVE-2024-6609)

Irvan Kurniawan discovered that Firefox did not properly manage memory during thread creation. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code.

(CVE-2024-6603)

It was discovered that Firefox incorrectly handled array accesses in the clipboard component, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-6606)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6890-1>

Solution

Update the affected 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-2024-6601 |
| CVE | CVE-2024-6602 |
| CVE | CVE-2024-6603 |
| CVE | CVE-2024-6604 |
| CVE | CVE-2024-6606 |
| CVE | CVE-2024-6607 |
| CVE | CVE-2024-6608 |
| CVE | CVE-2024-6609 |
| CVE | CVE-2024-6610 |
| CVE | CVE-2024-6611 |
| CVE | CVE-2024-6612 |
| CVE | CVE-2024-6613 |
| CVE | CVE-2024-6614 |
| CVE | CVE-2024-6615 |
| XREF | USN:6890-1 |
| XREF | IAVA:2024-A-0386-S |

Plugin Information

Published: 2024/07/10, Modified: 2025/07/17

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_128.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_128.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_128.0+build2-0ubuntu0.20.04.1

205779 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6966-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6966-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-7518, CVE-2024-7521, CVE-2024-7524, CVE-2024-7526, CVE-2024-7527, CVE-2024-7528, CVE-2024-7529, CVE-2024-7530, CVE-2024-7531)

It was discovered that Firefox did not properly manage certain memory operations when processing graphics shared memory. An attacker could potentially exploit this issue to escape the sandbox. (CVE-2024-7519)

Nan Wang discovered that Firefox did not properly handle type check in WebAssembly. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2024-7520)

Irvan Kurniawan discovered that Firefox did not properly check an attribute value in the editor component, leading to an out-of-bounds read vulnerability. An

attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-7522)

Rob Wu discovered that Firefox did not properly check permissions when creating a StreamFilter. An attacker could possibly use this issue to modify response body of requests on any site using a web extension. (CVE-2024-7525)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6966-1>

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-7518 |
| CVE | CVE-2024-7519 |
| CVE | CVE-2024-7520 |
| CVE | CVE-2024-7521 |
| CVE | CVE-2024-7522 |
| CVE | CVE-2024-7524 |
| CVE | CVE-2024-7525 |
| CVE | CVE-2024-7526 |
| CVE | CVE-2024-7527 |
| CVE | CVE-2024-7528 |
| CVE | CVE-2024-7529 |
| CVE | CVE-2024-7530 |
| CVE | CVE-2024-7531 |
| XREF | USN:6966-1 |
| XREF | IAVA:2024-A-0465-S |

Plugin Information

Published: 2024/08/19, Modified: 2024/09/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_129.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_129.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_129.0.1+build1-0ubuntu0.20.04.1

206626 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6992-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6992-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-8382, CVE-2024-8383, CVE-2024-8386, CVE-2024-8387, CVE-2024-8389)

Nils Bars discovered that Firefox contained a type confusion vulnerability when performing certain property name lookups. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-8381)

It was discovered that Firefox did not properly manage memory during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-8384)

Seunghyun Lee discovered that Firefox contained a type confusion

vulnerability when handling certain ArrayTypes. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-8385)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6992-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-8381 |
| CVE | CVE-2024-8382 |
| CVE | CVE-2024-8383 |
| CVE | CVE-2024-8384 |
| CVE | CVE-2024-8385 |
| CVE | CVE-2024-8386 |
| CVE | CVE-2024-8387 |
| CVE | CVE-2024-8389 |
| XREF | USN:6992-1 |
| XREF | IAVA:2024-A-0538-S |

Plugin Information

Published: 2024/09/05, Modified: 2025/02/03

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_130.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_130.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_130.0+build2-0ubuntu0.20.04.1
```

208230 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7056-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7056-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-9392, CVE-2024-9396, CVE-2024-9397, CVE-2024-9398, CVE-2024-9399, CVE-2024-9400, CVE-2024-9401, CVE-2024-9402, CVE-2024-9403)

Masato Kinugawa discovered that Firefox did not properly validate javascript under the resource://pdf.js origin. An attacker could potentially exploit this issue to execute arbitrary javascript code and access cross-origin PDF content. (CVE-2024-9393)

Masato Kinugawa discovered that Firefox did not properly validate javascript under the resource://devtools origin. An attacker could potentially exploit this issue to execute arbitrary javascript code and access cross-origin JSON content. (CVE-2024-9394)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7056-1>

Solution

Update the affected packages.

Risk Factor

Critical

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|-------------------------------|
| CVE | CVE-2024-9392 |
| CVE | CVE-2024-9393 |
| CVE | CVE-2024-9394 |
| CVE | CVE-2024-9396 |
| CVE | CVE-2024-9397 |
| CVE | CVE-2024-9398 |
| CVE | CVE-2024-9399 |
| CVE | CVE-2024-9400 |
| CVE | CVE-2024-9401 |
| CVE | CVE-2024-9402 |

| | |
|------|------------------------------------|
| CVE | CVE-2024-9403 |
| XREF | USN:7056-1 |
| XREF | IAVA:2024-A-0607-S |

Plugin Information

Published: 2024/10/07, Modified: 2024/11/04

Plugin Output

tcp/0

- Installed package : `firefox_78.0.2+build2-0ubuntu0.20.04.1`
- Fixed package : `firefox_131.0+build1.1-0ubuntu0.20.04.1`
- Installed package : `firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1`
- Fixed package : `firefox-locale-de_131.0+build1.1-0ubuntu0.20.04.1`
- Installed package : `firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1`
- Fixed package : `firefox-locale-en_131.0+build1.1-0ubuntu0.20.04.1`

[209983 - Ubuntu 20.04 LTS : Firefox vulnerabilities \(USN-7086-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7086-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-10458 CVE-2024-10459, CVE-2024-10460, CVE-2024-10461, CVE-2024-10462, CVE-2024-10463, CVE-2024-10464, CVE-2024-10465, CVE-2024-10466, CVE-2024-10467, CVE-2024-10468)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7086-1>

Solution

Update the affected 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

7.7 (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)

STIG Severity

I

References

| | |
|-----|--------------------------------|
| CVE | CVE-2024-10458 |
| CVE | CVE-2024-10459 |
| CVE | CVE-2024-10460 |
| CVE | CVE-2024-10461 |
| CVE | CVE-2024-10462 |
| CVE | CVE-2024-10463 |

| | |
|------|--------------------|
| CVE | CVE-2024-10464 |
| CVE | CVE-2024-10465 |
| CVE | CVE-2024-10466 |
| CVE | CVE-2024-10467 |
| CVE | CVE-2024-10468 |
| XREF | USN:7086-1 |
| XREF | IAVA:2024-A-0695-S |

Plugin Information

Published: 2024/10/31, Modified: 2024/12/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_132.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_132.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_132.0+build1-0ubuntu0.20.04.1

212017 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7134-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7134-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-11692, CVE-2024-11694, CVE-2024-11695, CVE-2024-11696, CVE-2024-11697, CVE-2024-11699, CVE-2024-11701, CVE-2024-11704, CVE-2024-11705, CVE-2024-11706, CVE-2024-11708)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7134-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|----------------|
| CVE | CVE-2024-11692 |
| CVE | CVE-2024-11694 |

| | |
|------|--------------------|
| CVE | CVE-2024-11695 |
| CVE | CVE-2024-11696 |
| CVE | CVE-2024-11697 |
| CVE | CVE-2024-11699 |
| CVE | CVE-2024-11701 |
| CVE | CVE-2024-11704 |
| CVE | CVE-2024-11705 |
| CVE | CVE-2024-11706 |
| CVE | CVE-2024-11708 |
| XREF | USN:7134-1 |
| XREF | IAVA:2024-A-0769-S |
| XREF | IAVA:2025-A-0079-S |

Plugin Information

Published: 2024/12/03, Modified: 2025/03/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_133.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_133.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_133.0+build2-0ubuntu0.20.04.1

216055 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7263-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7263-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2025-1011, CVE-2025-1013, CVE-2025-1014, CVE-2025-1016, CVE-2025-1017, CVE-2025-1018, CVE-2025-1019, CVE-2025-1020)

Ivan Fratric discovered that Firefox did not properly handle XSLT data, leading to a use-after-free vulnerability. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2025-1009)

Atte Kettunen discovered that Firefox did not properly manage memory in the Custom Highlight API, leading to a use-after-free vulnerability. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2025-1010)

Nils Bars discovered that Firefox did not properly manage memory during concurrent delazification, leading to a use-after-free vulnerability. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2025-1012)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7263-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-1009 |
| CVE | CVE-2025-1010 |
| CVE | CVE-2025-1011 |
| CVE | CVE-2025-1012 |
| CVE | CVE-2025-1013 |
| CVE | CVE-2025-1014 |
| CVE | CVE-2025-1016 |
| CVE | CVE-2025-1017 |
| CVE | CVE-2025-1018 |
| CVE | CVE-2025-1019 |
| CVE | CVE-2025-1020 |
| XREF | USN:7263-1 |
| XREF | IAVA:2025-A-0079-S |

Plugin Information

Published: 2025/02/11, Modified: 2025/03/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_135.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_135.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_135.0+build2-0ubuntu0.20.04.1

232218 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7334-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7334-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2025-1933, CVE-2025-1934, CVE-2025-1935, CVE-2025-1936, CVE-2025-1937, CVE-2025-1942)

It was discovered that Firefox did not properly handle WebTransport connection, leading to a use-after-free vulnerability. An attacker could potentially exploit this issue to cause a denial of service.

(CVE-2025-1931)

Ivan Fratric discovered that Firefox did not properly handle XSLT sorting, leading to a out-of-bounds access vulnerability. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2025-1932)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7334-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-1931 |
| CVE | CVE-2025-1932 |
| CVE | CVE-2025-1933 |
| CVE | CVE-2025-1934 |
| CVE | CVE-2025-1935 |
| CVE | CVE-2025-1936 |
| CVE | CVE-2025-1937 |
| CVE | CVE-2025-1942 |
| XREF | USN:7334-1 |
| XREF | IAVA:2025-A-0146-S |

Plugin Information

Published: 2025/03/06, Modified: 2025/04/03

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_136.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_136.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_136.0+build3-0ubuntu0.20.04.1

178207 - Ubuntu 20.04 LTS : Firefox vulnerability (USN-6218-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6218-1 advisory.

A use-after-free was discovered in Firefox when handling workers. An attacker could potentially exploit this to cause a denial of service, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6218-1>

Solution

Update the affected 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

7.7 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-3600 |
| XREF | USN:6218-1 |
| XREF | IAVA:2023-A-0337-S |

Plugin Information

Published: 2023/07/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_115.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_115.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_115.0.2+build1-0ubuntu0.20.04.1

181410 - Ubuntu 20.04 LTS : Firefox vulnerability (USN-6367-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6367-1 advisory.

It was discovered that Firefox did not properly manage memory when handling WebP images. If a user were tricked into opening a webpage containing malicious WebP image file, an attacker could potentially exploit these to cause a denial of service or execute arbitrary code. (CVE-2023-4863)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6367-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-4863 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/04 |
| XREF | USN:6367-1 |
| XREF | IAVA:2023-A-0491-S |

Plugin Information

Published: 2023/09/14, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_117.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_117.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_117.0.1+build2-0ubuntu0.20.04.1

208937 - Ubuntu 20.04 LTS : Firefox vulnerability (USN-7065-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7065-1 advisory.

Damien Schaeffer discovered that Firefox did not properly manage memory in the content process when handling Animation timelines, leading to a use after free vulnerability. An attacker could possibly use this issue to achieve remote code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7065-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2024-9680 |
| XREF | USN:7065-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/11/05 |
| XREF | IAVA:2024-A-0641-S |

Plugin Information

Published: 2024/10/14, Modified: 2024/12/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_131.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_131.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_131.0.2+build1-0ubuntu0.20.04.1

207055 - Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-7003-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7003-1 advisory.

It was discovered that the JFS file system contained an out-of-bounds read vulnerability when printing xattr debug information. A local attacker could use this to cause a denial of service (system crash).

(CVE-2024-40902)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- MIPS architecture;
- PowerPC architecture;
- x86 architecture;
- ACPI drivers;
- Serial ATA and Parallel ATA drivers;
- Drivers core;
- GPIO subsystem;
- GPU drivers;
- Greybus drivers;
- HID subsystem;
- I2C subsystem;
- IIO subsystem;
- InfiniBand drivers;

- Media drivers;
- VMware VMCI Driver;
- Network drivers;
- Pin controllers subsystem;
- S/390 drivers;
- SCSI drivers;
- USB subsystem;
- JFFS2 file system;
- JFS file system;
- File systems infrastructure;
- NILFS2 file system;
- IOMMU subsystem;
- Sun RPC protocol;
- Netfilter;
- Memory management;
- B.A.T.M.A.N. meshing protocol;
- CAN network layer;
- Ceph Core library;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- IUCV driver;
- MAC80211 subsystem;
- NET/ROM layer;
- Network traffic control;
- SoC Audio for Freescale CPUs drivers; (CVE-2024-40905, CVE-2024-41095, CVE-2024-41035, CVE-2024-36974, CVE-2024-40959, CVE-2024-40978, CVE-2024-42236, CVE-2024-40963, CVE-2024-40916, CVE-2024-41006, CVE-2024-39495, CVE-2023-52803, CVE-2024-42070, CVE-2024-41041, CVE-2024-42157, CVE-2024-36894, CVE-2024-42153, CVE-2024-42127, CVE-2024-42224, CVE-2024-40932, CVE-2024-42105, CVE-2024-40968, CVE-2024-41044, CVE-2024-41046, CVE-2023-52887, CVE-2024-42094, CVE-2024-40960, CVE-2024-41007, CVE-2024-40961, CVE-2024-39487, CVE-2024-39502, CVE-2024-42086, CVE-2024-36978, CVE-2024-39503, CVE-2024-41049, CVE-2024-42090, CVE-2024-42232, CVE-2024-39499, CVE-2024-40902, CVE-2024-37078, CVE-2024-39501, CVE-2024-42119, CVE-2024-40901, CVE-2024-42101, CVE-2024-42104, CVE-2024-42145, CVE-2024-41097, CVE-2024-40942, CVE-2024-41034, CVE-2024-40904, CVE-2024-41089, CVE-2024-42084, CVE-2024-42093, CVE-2024-40945, CVE-2024-40958, CVE-2024-42124, CVE-2024-40987, CVE-2024-40912, CVE-2024-39506, CVE-2024-40941, CVE-2024-39509, CVE-2024-40974, CVE-2024-39505, CVE-2024-42115, CVE-2024-40988, CVE-2024-40995, CVE-2024-42097, CVE-2024-41087, CVE-2024-42106, CVE-2024-40984, CVE-2024-40981, CVE-2024-42102, CVE-2024-42148, CVE-2024-42154, CVE-2024-42096, CVE-2024-40934, CVE-2024-40980, CVE-2024-42076, CVE-2024-40943, CVE-2024-42092, CVE-2024-42089, CVE-2024-42223, CVE-2024-38619, CVE-2024-42087, CVE-2024-39469)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7003-1>

Solution

Update the affected kernel package.

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-2023-52803
CVE-2023-52887
CVE-2024-36894
CVE-2024-36974
CVE-2024-36978
CVE-2024-37078
CVE-2024-38619
CVE-2024-39469
CVE-2024-39487
CVE-2024-39495
CVE-2024-39499
CVE-2024-39501
CVE-2024-39502
CVE-2024-39503
CVE-2024-39505
CVE-2024-39506
CVE-2024-39509
CVE-2024-40901
CVE-2024-40902
CVE-2024-40904
CVE-2024-40905
CVE-2024-40912
CVE-2024-40916
CVE-2024-40932
CVE-2024-40934
CVE-2024-40941
CVE-2024-40942
CVE-2024-40943
CVE-2024-40945
CVE-2024-40958
CVE-2024-40959
CVE-2024-40960
CVE-2024-40961
CVE-2024-40963
CVE-2024-40968
CVE-2024-40974
CVE-2024-40978
CVE-2024-40980
CVE-2024-40981
CVE-2024-40984
CVE-2024-40987
CVE-2024-40988
CVE-2024-40995
CVE-2024-41006
CVE-2024-41007
CVE-2024-41034
CVE-2024-41035
CVE-2024-41041
CVE-2024-41044
CVE-2024-41046
CVE-2024-41049
CVE-2024-41087
CVE-2024-41089
CVE-2024-41095
CVE-2024-41097
CVE-2024-42070
CVE-2024-42076
CVE-2024-42084
CVE-2024-42086
CVE-2024-42087
CVE-2024-42089
CVE-2024-42090

CVE-CVE-2024-42092
CVE-CVE-2024-42093
CVE-CVE-2024-42094
CVE-CVE-2024-42096
CVE-CVE-2024-42097
CVE-CVE-2024-42101
CVE-CVE-2024-42102
CVE-CVE-2024-42104
CVE-CVE-2024-42105
CVE-CVE-2024-42106
CVE-CVE-2024-42115
CVE-CVE-2024-42119
CVE-CVE-2024-42124
CVE-CVE-2024-42127
CVE-CVE-2024-42145
CVE-CVE-2024-42148
CVE-CVE-2024-42153
CVE-CVE-2024-42154
CVE-CVE-2024-42157
CVE-CVE-2024-42223
CVE-CVE-2024-42224
CVE-CVE-2024-42232
CVE-CVE-2024-42236
XREF-USN:7003-1

Plugin Information

Published: 2024/09/12, Modified: 2024/09/12

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-195-generic for this advisory.

149417 - Ubuntu 20.04 LTS : PyYAML vulnerability (USN-4940-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4940-1 advisory.

It was discovered that PyYAML incorrectly handled untrusted YAML files with the FullLoader loader. A remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4940-1>

Solution

Update the affected python-yaml and / or python3-yaml 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-14343 |
| XREF | USN:4940-1 |
| XREF | IAVA:2021-A-0463 |

Plugin Information

Published: 2021/05/12, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : python3-yaml_5.3.1-1
- Fixed package : python3-yaml_5.3.1-1ubuntu0.1

[172367 - Ubuntu 20.04 LTS : Samba vulnerabilities \(USN-5936-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5936-1 advisory.

Evgeny Legerov discovered that Samba incorrectly handled buffers in certain GSSAPI routines of Heimdal. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service.

(CVE-2022-3437)

Tom Tervoort discovered that Samba incorrectly used weak rc4-hmac Kerberos keys. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-37966, CVE-2022-37967)

It was discovered that Samba supported weak RC4/HMAC-MD5 in NetLogon Secure Channel. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-38023)

Greg Hudson discovered that Samba incorrectly handled PAC parsing. On 32-bit systems, a remote attacker could use this issue to escalate privileges, or possibly execute arbitrary code. (CVE-2022-42898)

Joseph Sutton discovered that Samba could be forced to issue rc4-hmac encrypted Kerberos tickets. A remote attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-45141)

WARNING: This update upgrades the version of Samba to 4.15.13. Please see the upstream release notes for important changes in the new version:

<https://www.samba.org/samba/history/samba-4.15.0.html>

In addition, the security fixes included in this new version introduce several important behavior changes which may cause compatibility problems interacting with systems still expecting the former behavior.

Please see the following upstream advisories for more information:

<https://www.samba.org/samba/security/CVE-2022-37966.html> <https://www.samba.org/samba/security/CVE-2022-37967.html>
<https://www.samba.org/samba/security/CVE-2022-38023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5936-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-3437 |
| CVE | CVE-2022-37966 |
| CVE | CVE-2022-37967 |
| CVE | CVE-2022-38023 |
| CVE | CVE-2022-42898 |
| CVE | CVE-2022-45141 |
| XREF | USN:5936-1 |
| XREF | IAVA:2022-A-0447-S |
| XREF | IAVA:2022-A-0495-S |
| XREF | IAVA:2023-A-0004-S |

Plugin Information

Published: 2023/03/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libsmbclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmbclient_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.15.13+dfsg-0ubuntu0.20.04.1

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.15.13+dfsg-0ubuntu0.20.04.1
```

160307 - Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5394-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5394-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5394-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-22624 |
| CVE | CVE-2022-22628 |
| CVE | CVE-2022-22629 |
| CVE | CVE-2022-22637 |
| XREF | USN:5394-1 |

Plugin Information

Published: 2022/04/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.0-0ubuntu0.20.04.3

- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.0-0ubuntu0.20.04.3

- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.0-0ubuntu0.20.04.3

- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.0-0ubuntu0.20.04.3
```

42411 - Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.

Description

The remote host has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, right click on each share, go to the 'Sharing' tab, and click on 'Permissions'.

Risk Factor

High

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

| | |
|-----|---------------|
| BID | 8026 |
| CVE | CVE-1999-0519 |
| CVE | CVE-1999-0520 |

Plugin Information

Published: 2009/11/06, Modified: 2025/02/26

Plugin Output

tcp/445/cifs

The following shares can be accessed using a NULL session :

- Notes - (readable)
- + Content of this share :
- ..
- Mail.txt

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

It was discovered that less mishandled newline characters in file names. If a user or automated system were tricked into opening specially crafted files, an attacker could possibly use this issue to execute arbitrary commands on the host.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6756-1>

Solution

Update the affected less package.

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

7.5 (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-2024-32487 |
| XREF | USN:6756-1 |

Plugin Information

Published: 2024/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : less_551-1ubuntu0.1
- Fixed package : less_551-1ubuntu0.3

202187 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities (USN-6891-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6891-1 advisory.

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2015-20107)

It was discovered that Python incorrectly used regular expressions vulnerable to catastrophic backtracking. A remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-1060, CVE-2018-1061)

It was discovered that Python failed to initialize Expats hash salt. A remote attacker could possibly use this issue to cause hash collisions, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-14647)

It was discovered that Python incorrectly handled certain pickle files. An attacker could possibly use this issue to consume memory, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS.

(CVE-2018-20406)

It was discovered that Python incorrectly validated the domain when handling cookies. An attacker could possibly trick Python into sending cookies to the wrong domain. This issue only affected Ubuntu 14.04 LTS.

(CVE-2018-20852)

Jonathan Birch and Panayiotis Panayiotou discovered that Python incorrectly handled Unicode encoding during NFC normalization. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9636, CVE-2019-10160)

It was discovered that Python incorrectly parsed certain email addresses. A remote attacker could possibly use this issue to trick Python applications into accepting email addresses that should be denied. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-16056)

It was discovered that the Python documentation XML-RPC server incorrectly handled certain fields. A remote attacker could use this issue to execute a cross-site scripting (XSS) attack. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-16935)

It was discovered that Python documentation had a misleading information. A security issue could be possibly caused by wrong assumptions of this information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-17514)

It was discovered that Python incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-18348)

It was discovered that Python incorrectly handled certain TAR archives. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2019-20907)

Colin Read and Nicolas Edet discovered that Python incorrectly handled parsing certain X509 certificates.

An attacker could possibly use this issue to cause Python to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-5010)

It was discovered that Python incorrectly handled certain ZIP files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9674)

It was discovered that Python incorrectly handled certain urls. A remote attacker could possibly use this issue to perform CRLF injection attacks. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9740, CVE-2019-9947)

Sihoon Lee discovered that Python incorrectly handled the local_file: scheme. A remote attacker could possibly use this issue to bypass blocklist mechanisms. This issue only affected Ubuntu 14.04 LTS.

(CVE-2019-9948)

It was discovered that Python incorrectly handled certain IP values. An attacker could possibly use this issue to cause a denial of service. This issue only affected

Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.
(CVE-2020-14422)

It was discovered that Python incorrectly handled certain character sequences. A remote attacker could possibly use this issue to perform CRLF injection. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2020-26116)

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. This issue only affected Ubuntu 14.04 LTS.
(CVE-2020-27619, CVE-2021-3177)

It was discovered that Python incorrectly handled certain HTTP requests. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2020-8492)

It was discovered that the Python stdlib ipaddress API incorrectly handled octal strings. A remote attacker could possibly use this issue to perform a wide variety of attacks, including bypassing certain access restrictions. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-29921)

David Schwrer discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-3426)

It was discovered that Python incorrectly handled certain RFCs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3733)

It was discovered that Python incorrectly handled certain server responses. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3737)

It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2021-4189)

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.
(CVE-2022-0391)

Devin Jeanpierre discovered that Python incorrectly handled sockets when the multiprocessing module was being used. A local attacker could possibly use this issue to execute arbitrary code and escalate privileges. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-42919)

It was discovered that Python incorrectly handled certain inputs. If a user or an automated system were tricked into running a specially crafted input, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS and Ubuntu 22.04 LTS.
(CVE-2022-45061, CVE-2023-24329)

It was discovered that Python incorrectly handled certain scripts. An attacker could possibly use this issue to execute arbitrary code or cause a crash. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48560)

It was discovered that Python incorrectly handled certain plist files. If a user or an automated system were tricked into processing a specially crafted plist file, an attacker could possibly use this issue to consume resources, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48564)

It was discovered that Python did not properly handle XML entity declarations in plist files. An attacker could possibly use this vulnerability to perform an XML External Entity (XXE) injection, resulting in a denial of service or information disclosure. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48565)

It was discovered that Python did not properly provide constant-time processing for a crypto operation. An attacker could possibly use this issue to perform a timing attack and recover sensitive information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48566)

It was discovered that Python instances of ssl.SSLSocket were vulnerable to a bypass of the TLS handshake.
An attacker could possibly use this issue to cause applications to treat unauthenticated received data before TLS handshake as authenticated data after TLS handshake. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-40217)

It was discovered that Python incorrectly handled null bytes when normalizing pathnames. An attacker could possibly use this issue to bypass certain filename checks. This issue only affected Ubuntu 22.04 LTS.
(CVE-2023-41105)

It was discovered that Python incorrectly handled privilege with certain parameters. An attacker could possibly use this issue to maintain the original processes' groups before starting the new process. This issue only affected Ubuntu 23.10. (CVE-2023-6507)

It was discovered that Python incorrectly handled symlinks in temp files. An attacker could possibly use this issue to modify the permissions of files. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-6597)

It was discovered that Python incorrectly handled certain crafted zip files. An attacker could possibly use this issue to crash the program, resulting in a denial of service. (CVE-2024-0450)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6891-1>

Solution

Update the affected 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/Vl: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

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-2018-1060 |
| CVE | CVE-2018-1061 |
| CVE | CVE-2018-14647 |
| CVE | CVE-2018-20406 |
| CVE | CVE-2018-20852 |
| CVE | CVE-2019-5010 |
| CVE | CVE-2019-9636 |
| CVE | CVE-2019-9674 |
| CVE | CVE-2019-9740 |
| CVE | CVE-2019-9947 |
| CVE | CVE-2019-9948 |
| CVE | CVE-2019-10160 |
| CVE | CVE-2019-16056 |
| CVE | CVE-2019-16935 |
| CVE | CVE-2019-17514 |
| CVE | CVE-2019-18348 |
| CVE | CVE-2019-20907 |
| CVE | CVE-2020-8492 |
| CVE | CVE-2020-14422 |
| CVE | CVE-2020-26116 |
| CVE | CVE-2020-27619 |
| CVE | CVE-2021-3177 |
| CVE | CVE-2021-3426 |
| CVE | CVE-2021-3733 |
| CVE | CVE-2021-3737 |
| CVE | CVE-2021-4189 |
| CVE | CVE-2021-29921 |
| CVE | CVE-2022-0391 |
| CVE | CVE-2022-42919 |
| CVE | CVE-2022-45061 |
| CVE | CVE-2022-48560 |
| CVE | CVE-2022-48564 |
| CVE | CVE-2022-48565 |
| CVE | CVE-2022-48566 |
| CVE | CVE-2023-6507 |
| CVE | CVE-2023-6597 |
| CVE | CVE-2023-24329 |
| CVE | CVE-2023-40217 |
| CVE | CVE-2023-41105 |
| CVE | CVE-2024-0450 |
| XREF | USN:6891-1 |

Plugin Information

Published: 2024/07/11, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.10
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.10
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.10
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.10
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.10

192219 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6698-1 advisory.

Zhen Zhou discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6698-1>

Solution

Update the affected 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-2024-22667 |
| XREF | USN:6698-1 |

Plugin Information

Published: 2024/03/18, Modified: 2025/02/06

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.22
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.22

- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.22

192938 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server vulnerabilities (USN-6721-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6721-1 advisory.

It was discovered that X.Org X Server incorrectly handled certain data. An attacker could possibly use this issue to expose sensitive information. (CVE-2024-31080, CVE-2024-31081, CVE-2024-31082)

It was discovered that X.Org X Server incorrectly handled certain glyphs. An attacker could possibly use this issue to cause a crash or expose sensitive information. (CVE-2024-31083)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6721-1>

Solution

Update the affected 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

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)

References

| | |
|------|----------------|
| CVE | CVE-2024-31080 |
| CVE | CVE-2024-31081 |
| CVE | CVE-2024-31082 |
| CVE | CVE-2024-31083 |
| XREF | USN:6721-1 |

Plugin Information

Published: 2024/04/05, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.16
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.16
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.16
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.16

- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.16

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6736-1 advisory.

It was discovered that zlib, vendored in klibc, incorrectly handled pointer arithmetic. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2016-9840, CVE-2016-9841)

Danilo Ramos discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2018-25032)

Evgeny Legerov discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2022-37434)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6736-1>

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev 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-2016-9840 |
| CVE | CVE-2016-9841 |
| CVE | CVE-2018-25032 |
| CVE | CVE-2022-37434 |
| XREF | USN:6736-1 |

Plugin Information

Published: 2024/04/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : klibc-utils_2.0.7-1ubuntu5
- Fixed package : klibc-utils_2.0.7-1ubuntu5.2
- Installed package : libklibc_2.0.7-1ubuntu5
- Fixed package : libklibc_2.0.7-1ubuntu5.2

237449 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Setuptools vulnerability (USN-7544-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7544-1 advisory.

It was discovered that setuptools did not properly sanitize paths. An attacker could possibly use this issue to write files to arbitrary locations on the filesystem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7544-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

8.7 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:N/V:I:H/V/A:N/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:H/A:N)

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:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2025-47273 |
| XREF | USN:7544-1 |

Plugin Information

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

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : python3-pkg-resources_45.2.0-1
- Fixed package : python3-pkg-resources_45.2.0-1ubuntu0.3

214997 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerability (USN-7257-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7257-1 advisory.

Goldberg, Miro Haller, Nadia Heninger, Mike Milano, Dan Shumow, Marc Stevens, and Adam Suhl discovered that Kerberos incorrectly authenticated certain responses. An attacker able to intercept communications between a RADIUS client and server could possibly use this issue to forge responses, bypass authentication, and access network devices and services.

This update introduces support for the Message-Authenticator attribute in non-EAP authentication methods for communications between Kerberos and a RADIUS server.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7257-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

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

7.8 (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-2024-3596 |
| XREF | USN:7257-1 |

Plugin Information

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

Plugin Output

tcp/0

```
- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.8

- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.8

- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.8

- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.8

- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.8
```

205195 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerabilities (USN-6947-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6947-1 advisory.

It was discovered that Kerberos incorrectly handled GSS message tokens where an unwrapped token could appear to be truncated. An attacker could possibly use this issue to cause a denial of service.

(CVE-2024-37370)

It was discovered that Kerberos incorrectly handled GSS message tokens when sent a token with invalid length fields. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-37371)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6947-1>

Solution

Update the affected 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

7.9 (CVSS:3.0/E:U/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

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

References

| | |
|------|----------------|
| CVE | CVE-2024-37370 |
| CVE | CVE-2024-37371 |
| XREF | USN:6947-1 |

Plugin Information

Published: 2024/08/08, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.6
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.6
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.6
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.6
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.6

241065 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libxslt vulnerability (USN-7600-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7600-1 advisory.

It was discovered that libxslt could be made to expose sensitive information about address space layout. An attacker could possibly use this issue to bypass Address Space Layout Randomization (ASLR) protections.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7600-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2023-40403
XREF-USN:7600-1

Plugin Information

Published: 2025/07/01, Modified: 2025/07/01

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : libxslt1.1_1.1.34-4
- Fixed package : libxslt1.1_1.1.34-4ubuntu0.20.04.3+esm1

190713 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 : LibTIFF vulnerabilities (USN-6644-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6644-1 advisory.

It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the application to crash, resulting in a denial of service. (CVE-2023-52356)

It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-6228)

It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the application to consume resources, resulting in a denial of service. (CVE-2023-6277)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6644-1>

Solution

Update the affected 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-2023-6228 |
| CVE | CVE-2023-6277 |
| CVE | CVE-2023-52356 |
| XREF | USN:6644-1 |

Plugin Information

Published: 2024/02/19, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.12

183889 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6452-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6452-1 advisory.

It was discovered that Vim could be made to divide by zero. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04. (CVE-2023-3896)

It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-4733, CVE-2023-4750)

It was discovered that Vim contained an arithmetic overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10.
(CVE-2023-4734)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-4735, CVE-2023-5344)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-4738)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-4751)

It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-4752, CVE-2023-5535)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-4781)

It was discovered that Vim could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-5441)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6452-1>

Solution

Update the affected 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-2023-3896 |
| CVE | CVE-2023-4733 |
| CVE | CVE-2023-4734 |
| CVE | CVE-2023-4735 |
| CVE | CVE-2023-4738 |
| CVE | CVE-2023-4750 |
| CVE | CVE-2023-4751 |
| CVE | CVE-2023-4752 |
| CVE | CVE-2023-4781 |
| CVE | CVE-2023-5344 |
| CVE | CVE-2023-5441 |
| CVE | CVE-2023-5535 |
| XREF | IAVB:2023-B-0066-S |
| XREF | IAVB:2023-B-0074-S |
| XREF | USN:6452-1 |
| XREF | IAVB:2023-B-0084-S |
| XREF | IAVA:2023-A-0579-S |

Plugin Information

Published: 2023/10/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.20

- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.20

- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.20
```

184303 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libsndfile vulnerability (USN-6471-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6471-1 advisory.

It was discovered that libsndfile contained multiple arithmetic overflows. If a user or automated system were tricked into processing a specially crafted audio file, an attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6471-1>

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs 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-2022-33065 |
| XREF | USN:6471-1 |

Plugin Information

Published: 2023/11/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsndfile1_1.0.28-7
- Fixed package : libsndfile1_1.0.28-7ubuntu0.2
```

185342 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : urllib3 vulnerabilities (USN-6473-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6473-1 advisory.

It was discovered that urllib3 didn't strip HTTP Authorization header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-25091)

It was discovered that urllib3 didn't strip HTTP Cookie header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-43804)

It was discovered that urllib3 didn't strip HTTP body on status code 303 redirects under certain circumstances. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-45803)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6473-1>

Solution

Update the affected python-urllib3 and / or python3-urllib3 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/V/A: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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2018-25091 |
| CVE | CVE-2023-43804 |
| CVE | CVE-2023-45803 |
| XREF | USN:6473-1 |

Plugin Information

Published: 2023/11/07, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.25.8-2
- Fixed package : python3-urllib3_1.25.8-2ubuntu0.3

186676 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6541-1 advisory.

It was discovered that the GNU C Library was not properly handling certain memory operations. An attacker could possibly use this issue to cause a denial of service (application crash). (CVE-2023-4806, CVE-2023-4813)

It was discovered that the GNU C library was not properly implementing a fix for CVE-2023-4806 in certain cases, which could lead to a memory leak. An attacker could possibly use this issue to cause a denial of service (application crash). This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-5156)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6541-1>

Solution

Update the affected 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/Vl: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

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-2023-4806 |
| CVE | CVE-2023-4813 |
| CVE | CVE-2023-5156 |
| XREF | USN:6541-1 |

Plugin Information

Published: 2023/12/07, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.14
- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.14
- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.14
- Installed package : libc6-dev_2.31-0ubuntu9
- Fixed package : libc6-dev_2.31-0ubuntu9.14
- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.14

179893 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerabilities (USN-6290-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6290-1 advisory.

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files with the tiffcrop utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-48281)

It was discovered that LibTIFF incorrectly handled certain image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04. (CVE-2023-2731)

It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-2908)

It was discovered that LibTIFF incorrectly handled certain file paths. If a user were tricked into specifying certain output paths, an attacker could possibly use this issue to cause a denial of service.

This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-3316)

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2023-3618)

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-25433, CVE-2023-26966)

It was discovered that LibTIFF did not properly managed memory when processing certain malformed image files with the tiffcrop utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-26965)

It was discovered that LibTIFF contained an arithmetic overflow. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service.

(CVE-2023-38288, CVE-2023-38289)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6290-1>

Solution

Update the affected 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-2022-48281

| | |
|------|----------------|
| CVE | CVE-2023-2731 |
| 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 |
| XREF | USN:6290-1 |

Plugin Information

Published: 2023/08/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.9

176714 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6139-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6139-1 advisory.

Yebo Cao discovered that Python incorrectly handled certain URLs. An attacker could use this issue to bypass blockinglisting methods. This issue was first addressed in USN-5960-1, but was incomplete. Here we address an additional fix to that issue. (CVE-2023-24329)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6139-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-24329 |
| XREF | USN:6139-1 |
| XREF | IAVA:2023-A-0283-S |

Plugin Information

Published: 2023/06/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.8
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.8
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.8
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.8
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.8

177108 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Vim vulnerabilities (USN-6154-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6154-1 advisory.

It was discovered that Vim was using uninitialized memory when fuzzy matching, which could lead to invalid memory access. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10 and Ubuntu 23.04. (CVE-2023-2426)

It was discovered that Vim was not properly performing bounds checks when processing register contents, which could lead to a NULL pointer dereference. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-2609)

It was discovered that Vim was not properly limiting the length of substitution expression strings, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-2610)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6154-1>

Solution

Update the affected 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-2023-2426 |
| CVE | CVE-2023-2609 |
| CVE | CVE-2023-2610 |
| XREF | USN:6154-1 |
| XREF | IAVB:2023-B-0033-S |
| XREF | IAVB:2023-B-0035-S |
| XREF | IAVB:2023-B-0039-S |

Plugin Information

Published: 2023/06/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.15
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.15
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.15

186225 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-6512-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6512-1 advisory.

It was discovered that LibTIFF could be made to run into an infinite loop. If a user or an automated system were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-40090)

It was discovered that LibTIFF could be made leak memory. If a user or an automated system were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. (CVE-2023-3576)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6512-1>

Solution

Update the affected 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-2022-40090 |
| CVE | CVE-2023-3576 |
| XREF | USN:6512-1 |

Plugin Information

Published: 2023/11/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.11

186209 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : poppler vulnerabilities (USN-6508-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6508-1 advisory.

It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-23804)

It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. (CVE-2022-37050, CVE-2022-37051, CVE-2022-37052, CVE-2022-38349)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6508-1>

Solution

Update the affected 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-2020-23804 |
| CVE | CVE-2022-37050 |
| CVE | CVE-2022-37051 |
| CVE | CVE-2022-37052 |
| CVE | CVE-2022-38349 |
| XREF | USN:6508-1 |

Plugin Information

Published: 2023/11/23, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.4

- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.4

- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.4

- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.4
```

181362 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : Ghostscript vulnerabilities (USN-6364-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6364-1 advisory.

It was discovered that Ghostscript incorrectly handled certain PDF files. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-21710)

It was discovered that Ghostscript incorrectly handled certain PDF files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-21890)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6364-1>

Solution

Update the affected 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-2020-21710 |
| CVE | CVE-2020-21890 |
| XREF | USN:6364-1 |
| XREF | IAVB:2023-B-0070-S |

Plugin Information

Published: 2023/09/13, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.10

- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.10

- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.10

- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.10
```

179941 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : poppler vulnerabilities (USN-6299-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6299-1 advisory.

It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. (CVE-2020-36023, CVE-2020-36024)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6299-1>

Solution

Update the affected 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-2020-36023 |
| CVE | CVE-2020-36024 |
| XREF | USN:6299-1 |

Plugin Information

Published: 2023/08/17, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.3

- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.3

- Installed package : libpoppler97_0.86.1-0ubuntu1
```

- Fixed package : libpoppler97_0.86.1-0ubuntu1.3
- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.3

176325 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : GNU binutils vulnerabilities (USN-6101-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6101-1 advisory.

It was discovered that GNU binutils incorrectly handled certain DWARF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 22.10.
(CVE-2023-1579)

It was discovered that GNU binutils did not properly verify the version definitions in zer0-lengthverdef table. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10 and Ubuntu 23.04. (CVE-2023-1972)

It was discovered that GNU binutils did not properly validate the size of length parameter in vms-alpha. An attacker could possibly use this issue to cause a crash or access sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2023-25584)

It was discovered that GNU binutils did not properly initialized the file_table field of struct module and the_bfd field of asymbol. An attacker could possibly use this issue to cause a crash. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.
(CVE-2023-25585, CVE-2023-25588)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6101-1>

Solution

Update the affected 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:I/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-1579 |
| CVE | CVE-2023-1972 |
| CVE | CVE-2023-25584 |
| CVE | CVE-2023-25585 |
| CVE | CVE-2023-25588 |
| XREF | USN:6101-1 |

Plugin Information

Published: 2023/05/24, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.5
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.5
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.5
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.5
- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.5
- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.5

162425 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5487-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5487-1 advisory.

It was discovered that Apache HTTP Server mod_proxy_ajp incorrectly handled certain crafted request. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

(CVE-2022-26377)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-28614)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash or expose sensitive information. (CVE-2022-28615)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-29404)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash. (CVE-2022-30522)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2022-30556)

It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to bypass IP based authentication. (CVE-2022-31813)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5487-1>

Solution

Update the affected 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

8.5 (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-2022-26377 |
| CVE | CVE-2022-28614 |
| CVE | CVE-2022-28615 |
| CVE | CVE-2022-29404 |
| CVE | CVE-2022-30522 |
| CVE | CVE-2022-30556 |
| CVE | CVE-2022-31813 |
| XREF | USN:5487-1 |
| XREF | IAVA:2022-A-0230-S |

Plugin Information

Published: 2022/06/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.12
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.12
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.12
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.12

169518 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Dnsmasq vulnerability (USN-5408-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5408-1 advisory.

Petr Menk and Richard Johnson discovered that Dnsmasq incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5408-1>

Solution

Update the affected 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-2022-0934 |
| XREF | USN:5408-1 |

Plugin Information

Published: 2023/01/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dnsmasq-base_2.80-1.1ubuntu1
- Fixed package : dnsmasq-base_2.80-1.1ubuntu1.5

174553 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Dnsmasq vulnerability (USN-6034-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6034-1 advisory.

It was discovered that Dnsmasq was sending large DNS messages over UDP, possibly causing transmission failures due to IP fragmentation. This update lowers the default maximum size of DNS messages to improve transmission reliability over UDP.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6034-1>

Solution

Update the affected 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-2023-28450 |
| XREF | USN:6034-1 |

Plugin Information

Published: 2023/04/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dnsmasq-base_2.80-1.1ubuntu1
- Fixed package : dnsmasq-base_2.80-1.1ubuntu1.7

168153 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerability (USN-5638-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5638-3 advisory.

USN-5638-1 fixed a vulnerability in Expat. This update provides the corresponding updates for Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-43680) This update also fixes a minor regression introduced in Ubuntu 18.04 LTS.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5638-3>

Solution

Update the affected 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
XREF

[CVE-2022-43680](#)
[USN:5638-3](#)

Plugin Information

Published: 2022/11/23, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.6

171928 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerabilities (USN-5886-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5886-1 advisory.

Erik C. Bjorge discovered that some Intel(R) Atom and Intel Xeon Scalable Processors did not properly implement access controls for out-of-band management. This may allow a privileged network-adjacent user to potentially escalate privileges. (CVE-2022-21216)

Cfir Cohen, Erdem Aktas, Felix Wilhelm, James Forshaw, Josh Eads, Nagaraju Kodalapura Nagabhushana Rao, Przemyslaw Duda, Liron Shacham and Ron Anderson discovered that some Intel(R) Xeon(R) Processors used incorrect default permissions in some memory controller configurations when using Intel(R) Software Guard Extensions. This may allow a privileged local user to potentially escalate privileges. (CVE-2022-33196)

It was discovered that some 3rd Generation Intel(R) Xeon(R) Scalable Processors did not properly calculate microkey keying. This may allow a privileged local user to potentially disclose information.

(CVE-2022-33972)

Joseph Nuzman discovered that some Intel(R) Processors when using Intel(R) Software Guard Extensions did not properly isolate shared resources. This may allow a privileged local user to potentially disclose information. (CVE-2022-38090)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5886-1>

Solution

Update the affected intel-microcode package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-21216 |
| CVE | CVE-2022-33196 |
| CVE | CVE-2022-33972 |
| CVE | CVE-2022-38090 |
| XREF | USN:5886-1 |

Plugin Information

Published: 2023/02/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20230214.0ubuntu0.20.04.1

167166 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5714-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5714-1 advisory.

It was discovered that LibTIFF incorrectly handled certain memory operations when using tiffcrop. An attacker could trick a user into processing a specially crafted tiff image file and potentially use this issue to cause a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-2519, CVE-2022-2520, CVE-2022-2521, CVE-2022-2953)

It was discovered that LibTIFF did not properly perform bounds checking in certain operations when using tiffcrop. An attacker could trick a user into processing a specially crafted tiff image file and potentially use this issue to allow for information disclosure or to cause the application to crash. This issue only affected to Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2867, CVE-2022-2868, CVE-2022-2869)

It was discovered that LibTIFF did not properly perform bounds checking in certain operations when using tiffsplit. An attacker could trick a user into processing a specially crafted tiff image file and potentially use this issue to allow for information disclosure or to cause the application to crash. This issue only affected to Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-34526)

Chintan Shah discovered that LibTIFF incorrectly handled memory in certain conditions when using tiffcrop.

An attacker could trick a user into processing a specially crafted image file and potentially use this issue to allow for information disclosure or to cause the application to crash. This issue only affected to Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3570)

It was discovered that LibTIFF incorrectly handled memory in certain conditions when using tiffcrop. An attacker could trick a user into processing a specially crafted tiff file and potentially use this issue to cause a denial of service. This issue only affected to Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3598)

It was discovered that LibTIFF did not properly perform bounds checking in

certain operations when using tiffcrop. An attacker could trick a user into

processing a specially crafted tiff image file and potentially use this issue

to allow for information disclosure or to cause the application to crash. (CVE-2022-3599)

It was discovered that LibTIFF did not properly perform bounds checking in certain operations when using tiffcrop. An attacker could trick a user into processing a specially crafted tiff image file and potentially use this issue to allow for information disclosure or to cause the application to crash. This issue only affected to Ubuntu 22.10. (CVE-2022-3597, CVE-2022-3626, CVE-2022-3627)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5714-1>

Solution

Update the affected 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-2022-2519
CVE CVE-2022-2520
CVE CVE-2022-2521
CVE CVE-2022-2867
CVE CVE-2022-2868
CVE CVE-2022-2869
CVE CVE-2022-2953
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-2022-34526
XREF USN:5714-1

Plugin Information

Published: 2022/11/09, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.6

173861 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5996-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5996-1 advisory.

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-26767, CVE-2023-26768, CVE-2023-26769)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5996-1>

Solution

Update the affected 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-2023-26767
CVE CVE-2023-26768
CVE CVE-2023-26769

XREF

USN:5996-1

Plugin Information

Published: 2023/04/04, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : liblouis-data_3.12.0-3
- Fixed package : liblouis-data_3.12.0-3ubuntu0.2

- Installed package : liblouis20_3.12.0-3
- Fixed package : liblouis20_3.12.0-3ubuntu0.2

- Installed package : python3-louis_3.12.0-3
- Fixed package : python3-louis_3.12.0-3ubuntu0.2
```

165282 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Mako vulnerability (USN-5625-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5625-1 advisory.

It was discovered that Mako incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5625-1>

Solution

Update the affected python-mako and / or python3-mako 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-2022-40023
USN:5625-1

Plugin Information

Published: 2022/09/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : python3-mako_1.1.0+ds1-1ubuntu2
```

- Fixed package : python3-mako_1.1.0+ds1-1ubuntu2.1

163104 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-5519-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5519-1 advisory.

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5519-1>

Solution

Update the affected 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 |
| XREF | USN:5519-1 |

Plugin Information

Published: 2022/07/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.5
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.5
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.5
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.5
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.5

172632 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-5960-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5960-1 advisory.

Yebo Cao discovered that Python incorrectly handled certain URLs. An attacker could possibly use this issue to bypass blocklisting methods by supplying a URL that starts with blank characters.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5960-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-24329 |
| XREF | USN:5960-1 |
| XREF | IAVA:2023-A-0118-S |
| XREF | IAVA:2023-A-0283-S |

Plugin Information

Published: 2023/03/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.7
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.7
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.7
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.7
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.7

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5963-1 advisory.

It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-47024, CVE-2023-0049, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433)

It was discovered that Vim was not properly performing memory management

operations. An attacker could possibly use this issue to cause a denial

of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-0051)

It was discovered that Vim was not properly performing memory management

operations. An attacker could possibly use this issue to cause a denial

of service or execute arbitrary code. (CVE-2023-1170, CVE-2023-1175)

It was discovered that Vim was not properly performing memory management

operations. An attacker could possibly use this issue to cause a denial

of service or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-1264)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5963-1>

Solution

Update the affected 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-2022-47024 |
| CVE | CVE-2023-0049 |
| CVE | CVE-2023-0051 |
| CVE | CVE-2023-0054 |
| CVE | CVE-2023-0288 |
| CVE | CVE-2023-0433 |
| CVE | CVE-2023-1170 |
| CVE | CVE-2023-1175 |
| CVE | CVE-2023-1264 |

| | |
|------|--------------------|
| XREF | IAVB:2023-B-0016-S |
| XREF | IAVB:2023-B-0018-S |
| XREF | USN:5963-1 |

Plugin Information

Published: 2023/03/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.12
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.12
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.12

168152 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerabilities (USN-5740-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5740-1 advisory.

It was discovered that X.Org X Server incorrectly handled certain inputs. An attacker could use these issues to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5740-1>

Solution

Update the affected 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)

References

| | |
|------|---------------|
| CVE | CVE-2022-3550 |
| CVE | CVE-2022-3551 |
| XREF | USN:5740-1 |

Plugin Information

Published: 2022/11/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.4
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.4
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.4
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.4
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.4

164950 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : poppler vulnerability (USN-5606-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5606-1 advisory.

It was discovered that poppler incorrectly handled certain PDF. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5606-1>

Solution

Update the affected 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-2022-38784 |
| XREF | USN:5606-1 |
| XREF | IAVB:2022-B-0033-S |
| XREF | IAVB:2022-B-0039-S |
| XREF | IAVB:2022-B-0050-S |

Plugin Information

Published: 2022/09/12, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.1
- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.1
- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.1
- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.1

170898 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : python-future vulnerability (USN-5833-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5833-1 advisory.

Sebastian Chnelik discovered that python-future incorrectly handled certain HTTP header field. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5833-1>

Solution

Update the affected python-future and / or python3-future 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-2022-40899 |
| XREF | USN:5833-1 |

Plugin Information

Published: 2023/01/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-future_0.18.2-2
- Fixed package : python3-future_0.18.2-2ubuntu0.1

159982 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5380-1 advisory.

It was discovered that Bash did not properly drop privileges when the binary had the setuid bit enabled.
An attacker could possibly use this issue to escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5380-1>

Solution

Update the affected bash, bash-builtins and / or bash-static 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/Vl:H/VA:H/SC:N/SI:N/SA:N)

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

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-2019-18276 |
| XREF | USN:5380-1 |

Plugin Information

Published: 2022/04/20, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : bash_5.0-6ubuntu1.1
- Fixed package : bash_5.0-6ubuntu1.2

158212 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Expat vulnerabilities (USN-5288-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5288-1 advisory.

It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5288-1>

Solution

Update the affected 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

9.0 (CVSS2#AV:N/AC:L/Au:S/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 |
| CVE | CVE-2022-25235 |
| CVE | CVE-2022-25236 |
| XREF | USN:5288-1 |

Plugin Information

Published: 2022/02/21, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.2

158789 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Expat vulnerabilities and regression (USN-5320-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5320-1 advisory.

USN-5288-1 fixed several vulnerabilities in Expat. For CVE-2022-25236 it caused a regression and an additional patch was required. This update address this regression and several other vulnerabilities.

It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-25313)

It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-25314)

It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-25315)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5320-1>

Solution

Update the affected 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-2022-25313 |
| CVE | CVE-2022-25314 |
| CVE | CVE-2022-25315 |
| XREF | USN:5320-1 |

Plugin Information

Published: 2022/03/10, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.4

163923 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-5555-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5555-1 advisory.

It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-1920, CVE-2022-1921)

It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1922, CVE-2022-1923, CVE-2022-1924, CVE-2022-1925, CVE-2022-2122)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5555-1>

Solution

Update the affected 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-2022-1920 |
| CVE | CVE-2022-1921 |
| CVE | CVE-2022-1922 |
| CVE | CVE-2022-1923 |
| CVE | CVE-2022-1924 |
| CVE | CVE-2022-1925 |
| CVE | CVE-2022-2122 |
| XREF | USN:5555-1 |

Plugin Information

Published: 2022/08/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gstreamer1.0-gtk3_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-gtk3_1.16.3-0ubuntu1.1
- Installed package : gstreamer1.0-plugins-good_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-plugins-good_1.16.3-0ubuntu1.1
- Installed package : gstreamer1.0-pulseaudio_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-pulseaudio_1.16.3-0ubuntu1.1
- Installed package : libgstreamer-plugins-good1.0-0_1.16.2-1ubuntu2
- Fixed package : libgstreamer-plugins-good1.0-0_1.16.3-0ubuntu1.1

171212 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5849-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5849-1 advisory.

Helmut Grohne discovered that Heimdal GSSAPI incorrectly handled logical conditions that are related to memory management operations. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5849-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.5 (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:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-45142 |
| XREF | USN:5849-1 |

Plugin Information

Published: 2023/02/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1.4
- Installed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1.4

[168489 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerability \(USN-5766-1\)](#)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5766-1 advisory.

It was discovered that Heimdal did not properly manage memory when normalizing Unicode. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5766-1>

Solution

Update the affected 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-2022-41916
XREF USN:5766-1

Plugin Information

Published: 2022/12/08, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1.2

- Installed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1.2
```

170011 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5804-1 advisory.

It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43945)

Tams Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42896)

It was discovered that the Xen netback driver in the Linux kernel did not properly handle packets structured in certain ways. An attacker in a guest VM could possibly use this to cause a denial of service (host NIC availability). (CVE-2022-3643)

It was discovered that an integer overflow vulnerability existed in the Bluetooth subsystem in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2022-45934)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5804-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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-2022-3643 |
| CVE | CVE-2022-42896 |
| CVE | CVE-2022-43945 |
| CVE | CVE-2022-45934 |
| XREF | USN:5804-1 |

Plugin Information

Published: 2023/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-137-generic for this advisory.

159882 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5379-1 advisory.

It was discovered that klibc did not properly perform some mathematical operations, leading to an integer overflow. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31870)

It was discovered that klibc did not properly handle some memory allocations on 64 bit systems. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31871)

It was discovered that klbc did not properly handled some file sizes values on 32 bit systems. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31872)

It was discovered that klbc did not properly handled some memory allocations. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31873)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5379-1>

Solution

Update the affected klbc-utils, libklbc and / or libklbc-dev 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-31870 |
| CVE | CVE-2021-31871 |
| CVE | CVE-2021-31872 |
| CVE | CVE-2021-31873 |
| XREF | USN:5379-1 |

Plugin Information

Published: 2022/04/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : klbc-utils_2.0.7-1ubuntu5
- Fixed package : klbc-utils_2.0.7-1ubuntu5.1

- Installed package : libklbc_2.0.7-1ubuntu5
- Fixed package : libklbc_2.0.7-1ubuntu5.1
```

200128 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GDK-PixBuf vulnerability (USN-6806-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6806-1 advisory.

Pedro Ribeiro and Vitor Pedreira discovered that the GDK-PixBuf library did not properly handle certain ANI files. An attacker could use this flaw to cause GDK-PixBuf to crash, resulting in a denial of service, or to possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6806-1>

Solution

Update the affected 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-2022-48622
XREF USN:6806-1

Plugin Information

Published: 2024/06/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.5

- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.5

- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.5

- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.5
```

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.

It was discovered that GNU C Library nscd daemon contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33599)

It was discovered that GNU C Library nscd daemon did not properly check the cache content, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33600)

It was discovered that GNU C Library nscd daemon did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33601)

It was discovered that GNU C Library nscd daemon did not properly handle memory allocation, which could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33602)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6804-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

6.7 (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 | USN:6804-1 |
| XREF | IAVA:2025-A-0062 |

Plugin Information

Published: 2024/05/31, Modified: 2025/03/27

Plugin Output

tcp/0

- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.16
- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.16
- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.16
- Installed package : libc6-dev_2.31-0ubuntu9
- Fixed package : libc6-dev_2.31-0ubuntu9.16
- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.16

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6780-1 advisory.

Guido Vranken discovered that idna did not properly manage certain inputs, which could lead to significant resource consumption. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6780-1>

Solution

Update the affected pypy-idna, python-idna and / or python3-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-2024-3651
XREF USN:6780-1

Plugin Information

Published: 2024/05/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-idna_2.8-1
- Fixed package : python3-idna_2.8-1ubuntu0.1

193905 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6754-1 advisory.

It was discovered that nghttp2 incorrectly handled the HTTP/2 implementation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-9511, CVE-2019-9513)

It was discovered that nghttp2 incorrectly handled request cancellation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2023-44487)

It was discovered that nghttp2 could be made to process an unlimited number of HTTP/2 CONTINUATION frames.

A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. (CVE-2024-28182)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6754-1>

Solution

Update the affected 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/V/A: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2019-9511 |
| CVE | CVE-2019-9513 |
| CVE | CVE-2023-44487 |
| CVE | CVE-2024-28182 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/31 |
| XREF | USN:6754-1 |
| XREF | CEA-ID:CEA-2024-0004 |
| XREF | CEA-ID:CEA-2019-0643 |

Plugin Information

Published: 2024/04/25, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libnghttp2-14_1.40.0-1build1
- Fixed package : libnghttp2-14_1.40.0-1ubuntu0.3

235363 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libsoup vulnerabilities (USN-7490-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7490-1 advisory.

Tan Wei Chong discovered that libsoup incorrectly handled memory when parsing HTTP request headers. An attacker could possibly use this issue to send a maliciously crafted HTTP request to the server, causing a denial of service. (CVE-2025-32906)

Alon Zahavi discovered that libsoup incorrectly parsed video files. An attacker could possibly use this issue to send a maliciously crafted HTTP response back to the client, causing a denial of service, or leading to undefined behavior. (CVE-2025-32909)

Jan Raski discovered that libsoup incorrectly handled memory when parsing authentication headers. An attacker could possibly use this issue to send a maliciously crafted HTTP response back to the client, causing a denial of service. (CVE-2025-32910, CVE-2025-32912)

It was discovered that libsoup incorrectly handled data in the hash table data type. An attacker could possibly use this issue to send a maliciously crafted HTTP request to the server, causing a denial of service or remote code execution. (CVE-2025-32911)

Jan Raski discovered that libsoup incorrectly handled memory when parsing the content disposition HTTP header. An attacker could possibly use this issue to send maliciously crafted data to a client or server, causing a denial of service. (CVE-2025-32913)

Alon Zahavi discovered that libsoup incorrectly handled memory when parsing HTTP requests. An attacker could possibly use this issue to send a maliciously crafted HTTP request to the server, causing a denial of service or obtaining sensitive information. (CVE-2025-32914)

It was discovered that libsoup incorrectly handled memory when parsing quality-list headers. An attacker could possibly use this issue to send a maliciously crafted HTTP request to the server, causing a denial of service. (CVE-2025-46420)

Jan Raski discovered that libsoup did not strip authorization information upon redirects. An attacker could possibly use this issue to obtain sensitive information. (CVE-2025-46421)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7490-1>

Solution

Update the affected 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:N/A:H)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2025-32906 |
| CVE | CVE-2025-32909 |
| CVE | CVE-2025-32910 |
| CVE | CVE-2025-32911 |
| CVE | CVE-2025-32912 |
| CVE | CVE-2025-32913 |
| CVE | CVE-2025-32914 |
| CVE | CVE-2025-46420 |
| CVE | CVE-2025-46421 |
| XREF | USN:7490-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : gir1.2-soup-2.4_2.70.0-1
- Fixed package : gir1.2-soup-2.4_2.70.0-1ubuntu0.3
- Installed package : libsoup-gnome2.4-1_2.70.0-1
- Fixed package : libsoup-gnome2.4-1_2.70.0-1ubuntu0.3
- Installed package : libsoup2.4-1_2.70.0-1
- Fixed package : libsoup2.4-1_2.70.0-1ubuntu0.3

206788 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : LibTIFF vulnerability (USN-6997-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6997-1 advisory.

It was discovered that LibTIFF incorrectly handled memory. An attacker could possibly use this issue to cause the application to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6997-1>

Solution

Update the affected 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-2024-7006
USN:6997-1

Plugin Information

Published: 2024/09/09, Modified: 2024/09/09

Plugin Output

tcp/0

```
- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.14
```

200132 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-6809-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6809-1 advisory.

It was discovered that BlueZ could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3563)

It was discovered that BlueZ could be made to write out of bounds. If a user were tricked into connecting to a malicious device, an attacker could possibly use this

issue to cause a denial of service or execute arbitrary code. (CVE-2023-27349)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6809-1>

Solution

Update the affected 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-2022-3563 |
| CVE | CVE-2023-27349 |
| XREF | USN:6809-1 |

Plugin Information

Published: 2024/06/05, Modified: 2025/07/09

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.8
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.8
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.8
- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.8

200771 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : gdb vulnerabilities (USN-6842-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6842-1 advisory.

It was discovered that gdb incorrectly handled certain memory operations when parsing an ELF file. An attacker could possibly use this issue to cause a denial of service. This issue is the result of an incomplete fix for CVE-2020-16599. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-4285)

It was discovered that gdb incorrectly handled memory leading to a heap based buffer overflow. An attacker could use this

issue to cause a denial of service, or possibly execute

arbitrary code. This issue only affected Ubuntu 22.04 LTS.

(CVE-2023-1972)

It was discovered that gdb incorrectly handled memory leading to a stack overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected

Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

(CVE-2023-39128)

It was discovered that gdb had a use after free vulnerability under certain circumstances. An attacker could use this to cause

a denial of service or possibly execute arbitrary code. This issue

only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS

and Ubuntu 22.04 LTS. (CVE-2023-39129)

It was discovered that gdb incorrectly handled memory leading to a

heap based buffer overflow. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. This issue

only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-39130)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6842-1>

Solution

Update the affected 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-2022-4285 |
| CVE | CVE-2023-1972 |
| CVE | CVE-2023-39128 |
| CVE | CVE-2023-39129 |
| CVE | CVE-2023-39130 |
| XREF | USN:6842-1 |

Plugin Information

Published: 2024/06/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gdb_9.1-0ubuntu1
- Fixed package : gdb_9.2-0ubuntu1~20.04.2
- Installed package : gdbserver_9.1-0ubuntu1
- Fixed package : gdbserver_9.2-0ubuntu1~20.04.2

139596 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-4458-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4458-1 advisory.

Fabrice Perez discovered that the Apache mod_rewrite module incorrectly handled certain redirects. A remote attacker could possibly use this issue to perform redirects to an unexpected URL. (CVE-2020-1927)

Chamal De Silva discovered that the Apache mod_proxy_ftp module incorrectly handled memory when proxying to a malicious FTP server. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2020-1934)

Felix Wilhelm discovered that the HTTP/2 implementation in Apache did not properly handle certain Cache-Digest headers. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-9490)

Felix Wilhelm discovered that the Apache mod_proxy_uwsgi module incorrectly handled large headers. A remote attacker could use this issue to obtain sensitive information or possibly execute arbitrary code.

This issue only affected Ubuntu 20.04 LTS. (CVE-2020-11984)

Felix Wilhelm discovered that the HTTP/2 implementation in Apache did not properly handle certain logging statements. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-11993)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4458-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|----------------------|
| CVE | CVE-2020-11984 |
| CVE | CVE-2020-11993 |
| CVE | CVE-2020-1927 |
| CVE | CVE-2020-1934 |
| CVE | CVE-2020-9490 |
| XREF | USN:4458-1 |
| XREF | IAVA:2020-A-0376-S |
| XREF | CEA-ID:CEA-2021-0025 |
| XREF | CEA-ID:CEA-2021-0004 |

Plugin Information

Published: 2020/08/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.1

- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.1

- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.1

- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.1
```

146068 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4720-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4720-1 advisory.

Itai Greenhut discovered that Apport incorrectly parsed certain files in the /proc filesystem. A local attacker could use this issue to escalate privileges and run arbitrary code. (CVE-2021-25682, CVE-2021-25683)

Itai Greenhut discovered that Apport incorrectly handled opening certain special files. A local attacker could possibly use this issue to cause Apport to hang, resulting in a denial of service. (CVE-2021-25684)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4720-1>

Solution

Update the affected 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

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-2021-25682 |
| CVE | CVE-2021-25683 |
| CVE | CVE-2021-25684 |
| XREF | USN:4720-1 |

Plugin Information

Published: 2021/02/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.16
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.16
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.16
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.16

145078 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Dnsmasq vulnerabilities (USN-4698-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4698-1 advisory.

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled memory when sorting RRsets. A remote attacker could use this issue to cause Dnsmasq to hang, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-25681, CVE-2020-25687)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled extracting certain names. A remote attacker could use this issue to cause Dnsmasq to hang, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-25682, CVE-2020-25683)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly implemented address/port checks. A remote attacker could use this issue to perform a cache poisoning attack. (CVE-2020-25684)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly implemented query resource name checks. A remote attacker could use this issue to perform a cache poisoning attack. (CVE-2020-25685)

Moshe Kol and Shlomi Oberman discovered that Dnsmasq incorrectly handled multiple query requests for the same resource name. A remote attacker could use this issue to perform a cache poisoning attack.
(CVE-2020-25686)

It was discovered that Dnsmasq incorrectly handled memory during DHCP response creation. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2019-14834)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4698-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------------|
| CVE | CVE-2019-14834 |
| CVE | CVE-2020-25681 |
| CVE | CVE-2020-25682 |
| CVE | CVE-2020-25683 |
| CVE | CVE-2020-25684 |
| CVE | CVE-2020-25685 |
| CVE | CVE-2020-25686 |
| CVE | CVE-2020-25687 |
| XREF | USN:4698-1 |
| XREF | CEA-ID:CEA-2021-0003 |

Plugin Information

Published: 2021/01/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dnsmasq-base_2.80-1.1ubuntu1
- Fixed package : dnsmasq-base_2.80-1.1ubuntu1.2

139182 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4443-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4443-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass iframe sandbox restrictions, confuse the user, or execute arbitrary code.
(CVE-2020-6463, CVE-2020-6514, CVE-2020-15652, CVE-2020-15653, CVE-2020-15654, CVE-2020-15656, CVE-2020-15658, CVE-2020-15659)

It was discovered that redirected HTTP requests which are observed or modified through a web extension could bypass existing CORS checks. If a user were tricked in to installing a specially crafted extension, an attacker could potentially exploit this to obtain sensitive information across origins.
(CVE-2020-15655)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4443-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-15652 |
| CVE | CVE-2020-15653 |
| CVE | CVE-2020-15654 |
| CVE | CVE-2020-15655 |
| CVE | CVE-2020-15656 |
| CVE | CVE-2020-15658 |
| CVE | CVE-2020-15659 |
| CVE | CVE-2020-6463 |
| CVE | CVE-2020-6514 |
| XREF | USN:4443-1 |
| XREF | IAVA:2020-A-0344-S |

Plugin Information

Published: 2020/07/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_79.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_79.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_79.0+build1-0ubuntu0.20.04.1

144299 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4671-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4671-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass the CSS sanitizer, bypass security restrictions, spoof the URL bar, or execute arbitrary code. (CVE-2020-16042, CVE-2020-26971, CVE-2020-26972, CVE-2020-26793, CVE-2020-26974, CVE-2020-26976, CVE-2020-26978, CVE-2020-26979, CVE-2020-35113, CVE-2020-35114)

It was discovered that the proxy.onRequest API did not catch view-source URLs. If a user were tricked into installing an extension with the proxy permission and opening View Source, an attacker could potentially exploit this to obtain sensitive information. (CVE-2020-35111)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4671-1>

Solution

Update the affected 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)

STIG Severity

|

References

| | |
|------|--------------------|
| CVE | CVE-2020-16042 |
| CVE | CVE-2020-26971 |
| CVE | CVE-2020-26972 |
| CVE | CVE-2020-26973 |
| CVE | CVE-2020-26974 |
| CVE | CVE-2020-26976 |
| CVE | CVE-2020-26978 |
| CVE | CVE-2020-26979 |
| CVE | CVE-2020-35111 |
| CVE | CVE-2020-35113 |
| CVE | CVE-2020-35114 |
| XREF | USN:4671-1 |
| XREF | IAVA:2020-A-0575-S |
| XREF | IAVA:2021-A-0051-S |

Plugin Information

Published: 2020/12/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_84.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_84.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_84.0+build3-0ubuntu0.20.04.1

142730 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerability (USN-4625-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4625-1 advisory.

A use-after-free was discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could exploit this to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4625-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-26950 |
| XREF | USN:4625-1 |
| XREF | IAVA:2020-A-0531-S |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2020/11/11, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_82.0.3+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_82.0.3+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_82.0.3+build1-0ubuntu0.20.04.1

140450 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4489-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4489-1 advisory.

Or Cohen discovered that the AF_PACKET implementation in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4489-1>

Solution

Update the affected kernel package.

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-2020-14386 |
| XREF | USN:4489-1 |

Plugin Information

Published: 2020/09/09, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-47-generic for this advisory.

141937 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4604-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4604-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.22 in Ubuntu 20.04 LTS and Ubuntu 20.10. Ubuntu 16.04 LTS and Ubuntu 18.04 LTS have been updated to MySQL 5.7.32.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-32.html>

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-22.html>

<https://www.oracle.com/security-alerts/cpuoct2020.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4604-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2020-14672 |
| CVE | CVE-2020-14760 |

CVE-2020-14765
CVE-2020-14769
CVE-2020-14771
CVE-2020-14773
CVE-2020-14775
CVE-2020-14776
CVE-2020-14777
CVE-2020-14785
CVE-2020-14786
CVE-2020-14789
CVE-2020-14790
CVE-2020-14791
CVE-2020-14793
CVE-2020-14794
CVE-2020-14800
CVE-2020-14804
CVE-2020-14809
CVE-2020-14812
CVE-2020-14814
CVE-2020-14821
CVE-2020-14827
CVE-2020-14828
CVE-2020-14829
CVE-2020-14830
CVE-2020-14836
CVE-2020-14837
CVE-2020-14838
CVE-2020-14839
CVE-2020-14844
CVE-2020-14845
CVE-2020-14846
CVE-2020-14848
CVE-2020-14852
CVE-2020-14853
CVE-2020-14860
CVE-2020-14861
CVE-2020-14866
CVE-2020-14867
CVE-2020-14868
CVE-2020-14869
CVE-2020-14870
CVE-2020-14873
CVE-2020-14878
CVE-2020-14888
CVE-2020-14891
CVE-2020-14893
XREF

Plugin Information

Published: 2020/10/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.22-0ubuntu0.20.04.2

146044

Synopsis

The remote U

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USCN-4716-1.

advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.25 in Ubuntu 20.04 LTS and Ubuntu 22.04. Ubuntu 18.04 LTS and Ubuntu 16.04 LTS have

In addition to security fixes, the updated pack-

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-33.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-23.html>
<https://www.oracle.com/security-alerts/cpujan2021.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4716-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------------|
| CVE | CVE-2021-2002 |
| CVE | CVE-2021-2010 |
| CVE | CVE-2021-2011 |
| CVE | CVE-2021-2014 |
| CVE | CVE-2021-2021 |
| CVE | CVE-2021-2022 |
| CVE | CVE-2021-2024 |
| CVE | CVE-2021-2031 |
| CVE | CVE-2021-2032 |
| CVE | CVE-2021-2036 |
| CVE | CVE-2021-2038 |
| CVE | CVE-2021-2046 |
| CVE | CVE-2021-2048 |
| CVE | CVE-2021-2056 |
| CVE | CVE-2021-2058 |
| CVE | CVE-2021-2060 |
| CVE | CVE-2021-2061 |
| CVE | CVE-2021-2065 |
| CVE | CVE-2021-2070 |
| CVE | CVE-2021-2072 |
| CVE | CVE-2021-2076 |
| CVE | CVE-2021-2081 |
| CVE | CVE-2021-2087 |
| CVE | CVE-2021-2088 |
| CVE | CVE-2021-2122 |
| XREF | USN:4716-1 |
| XREF | CEA-ID:CEA-2021-0004 |

Plugin Information

Published: 2021/02/01, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.23-0ubuntu0.20.04.1

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4471-1 advisory.

Tobias Neitzel discovered that Net-SNMP incorrectly handled certain symlinks. An attacker could possibly use this issue to access sensitive information. (CVE-2020-15861)

It was discovered that Net-SNMP incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2020-15862)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4471-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-15861 |
| CVE | CVE-2020-15862 |
| XREF | USN:4471-1 |
| XREF | IAVA:2020-A-0384-S |

Plugin Information

Published: 2020/08/25, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : libsnmp-base_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp-base_5.8+dfsg-2ubuntu2.3
- Installed package : libsnmp35_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp35_5.8+dfsg-2ubuntu2.3

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4602-1 advisory.

ManhND discovered that Perl incorrectly handled certain regular expressions. In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-10543)

Hugo van der Sanden and Slaven Rezic discovered that Perl incorrectly handled certain regular expressions.

In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2020-10878)

Sergey Aleynikov discovered that Perl incorrectly handled certain regular expressions. In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2020-12723)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4602-1>

Solution

Update the affected packages.

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-2020-10543 |
| CVE | CVE-2020-10878 |
| CVE | CVE-2020-12723 |
| XREF | USN:4602-1 |
| XREF | CEA-ID:CEA-2021-0004 |
| XREF | CEA-ID:CEA-2021-0025 |

Plugin Information

Published: 2020/10/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libperl5.30_5.30.0-9build1
- Fixed package : libperl5.30_5.30.0-9ubuntu0.2
- Installed package : perl_5.30.0-9build1
- Fixed package : perl_5.30.0-9ubuntu0.2
- Installed package : perl-base_5.30.0-9build1
- Fixed package : perl-base_5.30.0-9ubuntu0.2
- Installed package : perl-modules-5.30_5.30.0-9build1
- Fixed package : perl-modules-5.30_5.30.0-9ubuntu0.2

147998 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-4763-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4763-1 advisory.

It was discovered that Pillow incorrectly handled certain Tiff image files. If a user or automated system were tricked into opening a specially-crafted Tiff file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2021-25289, CVE-2021-25291)

It was discovered that Pillow incorrectly handled certain Tiff image files. If a user or automated system were tricked into opening a specially-crafted Tiff file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-25290)

It was discovered that Pillow incorrectly handled certain PDF files. If a user or automated system were tricked into opening a specially-crafted PDF file, a remote attacker could cause Pillow to hang, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-25292)

It was discovered that Pillow incorrectly handled certain SGI image files. If a user or automated system were tricked into opening a specially-crafted SGI file, a remote attacker could possibly cause Pillow to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-25293)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that Pillow incorrectly handled certain BLP files. If a user or automated system were tricked into opening a specially-crafted BLP file, a remote attacker could possibly cause Pillow to consume resources, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-27921)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that Pillow incorrectly handled certain ICNS files. If a user or automated system were tricked into opening a specially-crafted ICNS file, a remote attacker could possibly cause Pillow to consume resources, resulting in a denial of service. (CVE-2021-27922)

Jiayi Lin, Luke Shaffer, Xinran Xie, and Akshay Ajayan discovered that Pillow incorrectly handled certain ICO files. If a user or automated system were tricked into opening a specially-crafted ICO file, a remote attacker could possibly cause Pillow to consume resources, resulting in a denial of service. (CVE-2021-27922)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4763-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|--------------------------------|
| CVE | CVE-2021-25289 |
| CVE | CVE-2021-25290 |
| CVE | CVE-2021-25291 |

| | |
|------|----------------|
| CVE | CVE-2021-25292 |
| CVE | CVE-2021-25293 |
| CVE | CVE-2021-27921 |
| CVE | CVE-2021-27922 |
| CVE | CVE-2021-27923 |
| XREF | USN:4763-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.3

147997 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-4754-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4754-1 advisory.

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. (CVE-2020-27619, CVE-2021-3177)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4754-1>

Solution

Update the affected 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-2020-27619 |
| CVE | CVE-2021-3177 |
| XREF | USN:4754-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.5-1~20.04.2

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.5-1~20.04.2

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.5-1~20.04.2

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.5-1~20.04.2

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.5-1~20.04.2
```

141112 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba update (USN-4559-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4559-1 advisory.

Tom Tervoort discovered that the Netlogon protocol implemented by Samba incorrectly handled the authentication scheme. A remote attacker could use this issue to forge an authentication token and steal the credentials of the domain admin.

While a previous security update fixed the issue by changing the server schannel setting to default to yes, instead of auto, which forced a secure netlogon channel, this update provides additional improvements.

For compatibility reasons with older devices, Samba now allows specifying an insecure netlogon configuration per machine. See the following link for examples:
<https://www.samba.org/samba/security/CVE-2020-1472.html>

In addition, this update adds additional server checks for the protocol attack in the client-specified challenge to provide some protection when 'server schannel = no/auto' and avoid the false-positive results when running the proof-of-concept exploit.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4559-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2020-1472 |
| XREF | USN:4559-1 |
| XREF | IAVA:2020-A-0438-S |

| | |
|------|---------------------------------|
| XREF | IAVA:0001-A-0647 |
| XREF | CISA-KNOWN-EXPLOITED:2020/09/21 |
| XREF | CISA-NCAS:AA22-011A |
| XREF | CEA-ID:CEA-2020-0129 |
| XREF | CEA-ID:CEA-2020-0101 |
| XREF | CEA-ID:CEA-2021-0025 |
| XREF | CEA-ID:CEA-2021-0008 |
| XREF | CEA-ID:CEA-2020-0121 |
| XREF | CEA-ID:CEA-2023-0016 |

Plugin Information

Published: 2020/10/02, Modified: 2024/11/29

Plugin Output

tcp/0

- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.5
- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.5

145463 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Sudo vulnerabilities (USN-4705-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4705-1 advisory.

It was discovered that Sudo incorrectly handled memory when parsing command lines. A local attacker could possibly use this issue to obtain unintended access to the administrator account. (CVE-2021-3156)

It was discovered that the Sudo sudoedit utility incorrectly handled checking directory permissions. A local attacker could possibly use this issue to bypass file permissions and determine if a directory exists or not.

(CVE-2021-23239)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4705-1>

Solution

Update the affected sudo and / or sudo-ldap 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-3156 |
| CVE | CVE-2021-23239 |
| XREF | USN:4705-1 |
| XREF | IAVA:2021-A-0053 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/27 |

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2021/01/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : sudo_1.8.31-1ubuntu1
- Fixed package : sudo_1.8.31-1ubuntu1.2

141301 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Vino vulnerabilities (USN-4573-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4573-1 advisory.

Nicolas Ruff discovered that Vino incorrectly handled large ClientCutText messages. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service. (CVE-2014-6053)

It was discovered that Vino incorrectly handled certain packet lengths. A remote attacker could possibly use this issue to obtain sensitive information, cause a denial of service, or execute arbitrary code.
(CVE-2018-7225)

Pavel Cheremushkin discovered that an information disclosure vulnerability existed in Vino when sending a ServerCutText message. An attacker could possibly use this issue to expose sensitive information.
(CVE-2019-15681)

It was discovered that Vino incorrectly handled region clipping. A remote attacker could possibly use this issue to cause Vino to crash, resulting in a denial of service. (CVE-2020-14397)

It was discovered that Vino incorrectly handled encodings. A remote attacker could use this issue to cause Vino to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-14402, CVE-2020-14403, CVE-2020-14404)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4573-1>

Solution

Update the affected vino package.

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

| | |
|------|----------------|
| BID | 70092 |
| BID | 103107 |
| CVE | CVE-2014-6053 |
| CVE | CVE-2018-7225 |
| CVE | CVE-2019-15681 |
| CVE | CVE-2020-14397 |
| CVE | CVE-2020-14402 |
| CVE | CVE-2020-14403 |
| CVE | CVE-2020-14404 |
| XREF | USN:4573-1 |

Plugin Information

Published: 2020/10/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vino_3.22.0-5ubuntu2
- Fixed package : vino_3.22.0-5ubuntu2.1

148495 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4905-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4905-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain lengths of Xinput extension ChangeFeedbackControl requests. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4905-1>

Solution

Update the affected 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-2021-3472 |
| XREF | USN:4905-1 |

Plugin Information

Published: 2021/04/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.9-2ubuntu1.2~20.04.2
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.9-2ubuntu1.2~20.04.2
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.9-2ubuntu1.2~20.04.2
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.9-2ubuntu1.2~20.04.2
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.9-2ubuntu1.2~20.04.2

142732 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libxif vulnerability (USN-4624-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4624-1 advisory.

It was discovered that libxif incorrectly handled certain inputs. An attacker could possibly use this issue to cause unexpected behaviours, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4624-1>

Solution

Update the affected libxif-dev and / or libxif12 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

8.5 (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-2020-0452 |
| XREF | USN:4624-1 |

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexif12_0.6.21-6ubuntu0.3
- Fixed package : libexif12_0.6.21-6ubuntu0.4

139783 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : sane-backends vulnerabilities (USN-4470-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4470-1 advisory.

Kritphong Mongkhonvanit discovered that sane-backends incorrectly handled certain packets. A remote attacker could possibly use this issue to obtain sensitive memory information. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-6318)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to execute arbitrary code. This issue only applied to Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-12861)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2020-12862, CVE-2020-12863)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to obtain sensitive information. This issue only applied to Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-12864)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to execute arbitrary code. (CVE-2020-12865)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause a denial of service. This issue only applied to Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-12866)

It was discovered that sane-backends incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause a denial of service. (CVE-2020-12867)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4470-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2017-6318 |
| CVE | CVE-2020-12861 |
| CVE | CVE-2020-12862 |
| CVE | CVE-2020-12863 |
| CVE | CVE-2020-12864 |
| CVE | CVE-2020-12865 |
| CVE | CVE-2020-12866 |
| CVE | CVE-2020-12867 |
| XREF | USN:4470-1 |

Plugin Information

Published: 2020/08/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsane_1.0.29-0ubuntu5
- Fixed package : libsane_1.0.29-0ubuntu5.1
- Installed package : libsane-common_1.0.29-0ubuntu5
- Fixed package : libsane-common_1.0.29-0ubuntu5.1
- Installed package : sane-utils_1.0.29-0ubuntu5
- Fixed package : sane-utils_1.0.29-0ubuntu5.1

146437 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : wpa_supplicant and hostapd vulnerabilities (USN-4734-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4734-1 advisory.

It was discovered that wpa_supplicant did not properly handle P2P (Wi-Fi Direct) group information in some situations, leading to a heap overflow. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-0326)

It was discovered that hostapd did not properly handle UPnP subscribe messages in some circumstances. An attacker could use this to cause a denial of service. (CVE-2020-12695)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4734-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-12695 |
| CVE | CVE-2021-0326 |
| XREF | USN:4734-1 |
| XREF | CEA-ID:CEA-2020-0050 |

Plugin Information

Published: 2021/02/11, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : wpasupplicant_2:2.9-1ubuntu4.1
- Fixed package : wpasupplicant_2:2.9-1ubuntu4.2

180004 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6302-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6302-1 advisory.

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2522, CVE-2022-2580, CVE-2022-2817, CVE-2022-2819, CVE-2022-2862, CVE-2022-2889, CVE-2022-2982, CVE-2022-3134)

It was discovered that Vim did not properly perform bounds checks in the diff mode in certain situations.

An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2598)

It was discovered that Vim did not properly perform bounds checks in certain situations. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS.
(CVE-2022-2816)

It was discovered that Vim incorrectly handled memory when skipping compiled code. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS.
(CVE-2022-2874)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3016, CVE-2022-3037)

It was discovered that Vim incorrectly handled memory when invalid line number on :for is ignored. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3099)

It was discovered that Vim incorrectly handled memory when passing invalid arguments to the assert_fails() method. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3153)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6302-1>

Solution

Update the affected 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-2022-2522 |
| CVE | CVE-2022-2580 |
| CVE | CVE-2022-2598 |
| CVE | CVE-2022-2816 |
| CVE | CVE-2022-2817 |
| CVE | CVE-2022-2819 |
| CVE | CVE-2022-2862 |
| CVE | CVE-2022-2874 |
| CVE | CVE-2022-2889 |
| CVE | CVE-2022-2982 |
| CVE | CVE-2022-3016 |
| CVE | CVE-2022-3037 |
| CVE | CVE-2022-3099 |
| CVE | CVE-2022-3134 |
| CVE | CVE-2022-3153 |
| XREF | IAVB:2022-B-0049-S |
| XREF | USN:6302-1 |

Plugin Information

Published: 2023/08/21, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.17
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.17
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.17

186743 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6548-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6548-1 advisory.

It was discovered that Spectre-BHB mitigations were missing for Ampere processors. A local attacker could potentially use this to expose sensitive information. (CVE-2023-3006)

It was discovered that the USB subsystem in the Linux kernel contained a race condition while handling device descriptors in certain situations, leading to a out-of-bounds read vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-37453)

Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate some attributes passed from userspace. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2023-39189)

Sunjoo Park discovered that the netfilter subsystem in the Linux kernel did not properly validate u32 packets content, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39192)

Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate SCTP data, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39193)

Lucas Leong discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel did not properly handle state filters, leading to an out- of-bounds read vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39194)

Kyle Zeng discovered that the IPv4 implementation in the Linux kernel did not properly handle socket buffers (skb) when performing IP routing in certain circumstances, leading to a null pointer dereference vulnerability. A privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-42754)

Alon Zahavi discovered that the NVMe-oF/TCP subsystem in the Linux kernel did not properly handle queue initialization failures in certain situations, leading to a use-after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-5178)

Budimir Markovic discovered that the perf subsystem in the Linux kernel did not properly handle event groups, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-5717)

It was discovered that the TLS subsystem in the Linux kernel did not properly perform cryptographic operations in some situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6176)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6548-1>

Solution

Update the affected kernel package.

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-2023-3006 |
| CVE | CVE-2023-5178 |
| CVE | CVE-2023-5717 |
| CVE | CVE-2023-6176 |
| CVE | CVE-2023-37453 |
| CVE | CVE-2023-39189 |
| CVE | CVE-2023-39192 |
| CVE | CVE-2023-39193 |
| CVE | CVE-2023-39194 |
| CVE | CVE-2023-42754 |
| XREF | USN:6548-1 |

Plugin Information

Published: 2023/12/11, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-169-generic for this advisory.

175283 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities (USN-6060-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6060-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.33 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.42.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-42.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-33.html>
<https://www.oracle.com/security-alerts/cpuapr2023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6060-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|--------------------------------|
| CVE | CVE-2023-21911 |
| CVE | CVE-2023-21912 |
| CVE | CVE-2023-21919 |
| CVE | CVE-2023-21920 |
| CVE | CVE-2023-21929 |
| CVE | CVE-2023-21933 |
| CVE | CVE-2023-21935 |
| CVE | CVE-2023-21940 |
| CVE | CVE-2023-21945 |
| CVE | CVE-2023-21946 |
| CVE | CVE-2023-21947 |
| CVE | CVE-2023-21953 |
| CVE | CVE-2023-21955 |

| | |
|------|----------------|
| CVE | CVE-2023-21962 |
| CVE | CVE-2023-21966 |
| CVE | CVE-2023-21972 |
| CVE | CVE-2023-21976 |
| CVE | CVE-2023-21977 |
| CVE | CVE-2023-21980 |
| XREF | CVE-2023-21982 |
| | USN:6060-1 |

Plugin Information

Published: 2023/05/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.33-0ubuntu0.20.04.1

176478 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : TeX Live vulnerability (USN-6115-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6115-1 advisory.

Max Chernoff discovered that LuaTeX (TeX Live) did not properly disable shell escape. An attacker could possibly use this issue to execute arbitrary shell commands.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6115-1>

Solution

Update the affected 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

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-2023-32700 |
| XREF | USN:6115-1 |

Plugin Information

Published: 2023/05/30, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libkpathsea6_2019.20190605.51237-3build2
- Fixed package : libkpathsea6_2019.20190605.51237-3ubuntu0.1

- Installed package : libsynctex2_2019.20190605.51237-3build2
- Fixed package : libsynctex2_2019.20190605.51237-3ubuntu0.1
```

175977 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : cups-filters vulnerability (USN-6083-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6083-1 advisory.

It was discovered that cups-filters incorrectly handled the beh CUPS backend. A remote attacker could possibly use this issue to cause the backend to stop responding or to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6083-1>

Solution

Update the affected 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 (CVSS:2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.0 (CVSS:2#E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2023-24805 |
| XREF | USN:6083-1 |

Plugin Information

Published: 2023/05/17, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : cups-browsed_1.27.4-1
- Fixed package : cups-browsed_1.27.4-1ubuntu0.2

- Installed package : cups-filters_1.27.4-1
- Fixed package : cups-filters_1.27.4-1ubuntu0.2

- Installed package : cups-filters-core-drivers_1.27.4-1
- Fixed package : cups-filters-core-drivers_1.27.4-1ubuntu0.2

- Installed package : libcupsfilters1_1.27.4-1
- Fixed package : libcupsfilters1_1.27.4-1ubuntu0.2

- Installed package : libfontembed1_1.27.4-1
- Fixed package : libfontembed1_1.27.4-1ubuntu0.2
```

175916 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6078-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6078-1 advisory.

Irvan Kurniawan discovered that libwebp incorrectly handled certain memory operations. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6078-1>

Solution

Update the affected 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:O/RC:C)

References

| | |
|------|-------------------------------|
| CVE | CVE-2023-1999 |
| XREF | USN:6078-1 |

Plugin Information

Published: 2023/05/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libwebp6_0.6.1-2
- Fixed package : libwebp6_0.6.1-2ubuntu0.20.04.2
- Installed package : libwebpdemux2_0.6.1-2
- Fixed package : libwebpdemux2_0.6.1-2ubuntu0.20.04.2
- Installed package : libwebpmux3_0.6.1-2
- Fixed package : libwebpdux3_0.6.1-2ubuntu0.20.04.2

191499 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : python-cryptography vulnerabilities (USN-6673-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6673-1 advisory.

Hubert Kario discovered that python-cryptography incorrectly handled errors returned by the OpenSSL API when processing incorrect padding in RSA PKCS#1 v1.5. A remote attacker could possibly use this issue to expose confidential or sensitive information. (CVE-2023-50782)

It was discovered that python-cryptography incorrectly handled memory operations when processing mismatched PKCS#12 keys. A remote attacker could possibly use this issue to cause python-cryptography to crash, leading to a denial of service. This issue only affected Ubuntu 23.10. (CVE-2024-26130)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6673-1>

Solution

Update the affected python-cryptography and / or python3-cryptography 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:H/I:N/A:N)

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-50782 |
| CVE | CVE-2024-26130 |
| XREF | USN:6673-1 |

Plugin Information

Published: 2024/03/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-cryptography_2.8-3
- Fixed package : python3-cryptography_2.8-3ubuntu0.3

211896 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7126-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7126-1 advisory.

It was discovered that libsoup ignored certain characters at the end of header names. A remote attacker could possibly use this issue to perform a HTTP request smuggling attack. (CVE-2024-52530)

It was discovered that libsoup did not correctly handle memory while performing UTF-8 conversions. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-52531)

It was discovered that libsoup could enter an infinite loop when reading certain websocket data. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-52532)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7126-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.3 (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:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-52530 |
| CVE | CVE-2024-52531 |
| CVE | CVE-2024-52532 |
| XREF | USN:7126-1 |

Plugin Information

Published: 2024/11/27, Modified: 2024/11/27

Plugin Output

tcp/0

- Installed package : gir1.2-soup-2.4_2.70.0-1
- Fixed package : gir1.2-soup-2.4_2.70.0-1ubuntu0.1
- Installed package : libsoup-gnome2.4-1_2.70.0-1
- Fixed package : libsoup-gnome2.4-1_2.70.0-1ubuntu0.1
- Installed package : libsoup2.4-1_2.70.0-1
- Fixed package : libsoup2.4-1_2.70.0-1ubuntu0.1

170927 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5839-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5839-1 advisory.

It was discovered that the Apache HTTP Server mod_dav module incorrectly handled certain If: request headers. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2006-20001)

ZeddYu_Lu discovered that the Apache HTTP Server mod_proxy_ajp module incorrectly interpreted certain HTTP Requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.
(CVE-2022-36760)

Dimas Fariski Setyawan Putra discovered that the Apache HTTP Server mod_proxy module incorrectly truncated certain response headers. This may result in later headers not being interpreted by the client.
(CVE-2022-37436)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5839-1>

Solution

Update the affected packages.

Risk Factor

High

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

7.8 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2006-20001 |
| CVE | CVE-2022-36760 |
| CVE | CVE-2022-37436 |
| XREF | USN:5839-1 |
| XREF | IAVA:2023-A-0047-S |

Plugin Information

Published: 2023/02/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.13
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.13
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.13
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.13

165290 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Bind vulnerabilities (USN-5626-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5626-1 advisory.

Yehuda Afek, Anat Bremler-Barr, and Shani Stajnrod discovered that Bind incorrectly handled large delegations. A remote attacker could possibly use this issue to reduce performance, leading to a denial of service. (CVE-2022-2795)

It was discovered that Bind incorrectly handled statistics requests. A remote attacker could possibly use this issue to obtain sensitive memory contents, or cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2881)

It was discovered that Bind incorrectly handled memory when processing certain Diffie-Hellman key exchanges. A remote attacker could use this issue to consume resources, leading to a denial of service.

This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2906)

Maksym Odintsev discovered that Bind incorrectly handled answers from cache when configured with a zero stale-answer-timeout. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3080)

It was discovered that Bind incorrectly handled memory when processing ECDSA DNSSEC verification. A remote attacker could use this issue to consume resources, leading to a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2022-38177)

It was discovered that Bind incorrectly handled memory when processing EDDSA DNSSEC verification. A remote attacker could use this issue to consume resources, leading to a denial of service. (CVE-2022-38178)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5626-1>

Solution

Update the affected 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

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-2795 |
| CVE | CVE-2022-2881 |
| CVE | CVE-2022-2906 |
| CVE | CVE-2022-3080 |
| CVE | CVE-2022-38177 |
| CVE | CVE-2022-38178 |
| XREF | USN:5626-1 |

Plugin Information

Published: 2022/09/21, Modified: 2024/09/19

Plugin Output

tcp/0

```
- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.11

- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.11

- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.11
```

161723 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : CUPS vulnerabilities (USN-5454-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5454-1 advisory.

Joshua Mason discovered that CUPS incorrectly handled the secret key used to access the administrative web interface. A remote attacker could possibly use this issue to open a session as an administrator and execute arbitrary code. (CVE-2022-26691)

It was discovered that CUPS incorrectly handled certain memory operations when handling IPP printing. A remote attacker could possibly use this issue to cause CUPS to crash, leading to a denial of service, or obtain sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

(CVE-2019-8842, CVE-2020-10001)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5454-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/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

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-2019-8842 |
| CVE | CVE-2020-10001 |
| CVE | CVE-2022-26691 |
| XREF | USN:5454-1 |

Plugin Information

Published: 2022/05/31, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.2
```

- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.2
- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.2
- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.2
- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.2
- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.2
- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.2
- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.2
- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.2
- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.2
- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.2

175537 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ceph vulnerabilities (USN-6063-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6063-1 advisory.

Mark Kirkwood discovered that Ceph incorrectly handled certain key lengths. An attacker could possibly use this issue to create non-random encryption keys. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-3979)

It was discovered that Ceph incorrectly handled the volumes plugin. An attacker could possibly use this issue to obtain access to any share. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-0670)

It was discovered that Ceph incorrectly handled crash dumps. A local attacker could possibly use this issue to escalate privileges to root. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-3650)

It was discovered that Ceph incorrectly handled URL processing on RGW backends. An attacker could possibly use this issue to cause RGW to crash, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3854)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6063-1>

Solution

Update the affected 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:H/A:N)

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:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2021-3979 |
| CVE | CVE-2022-0670 |
| CVE | CVE-2022-3650 |
| CVE | CVE-2022-3854 |
| XREF | USN:6063-1 |

Plugin Information

Published: 2023/05/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcephfs2_15.2.3-0ubuntu0.20.04.1
- Fixed package : libcephfs2_15.2.17-0ubuntu0.20.04.3
- Installed package : librados2_15.2.3-0ubuntu0.20.04.1
- Fixed package : librados2_15.2.17-0ubuntu0.20.04.3

162376 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Exempi vulnerabilities (USN-5483-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5483-1 advisory.

It was discovered that Exempi incorrectly handled certain media files. If a user or automated system were tricked into opening a specially crafted file, a remote attacker could cause Exempi to stop responding or crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5483-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/U: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2018-12648 |
| CVE | CVE-2021-36045 |
| CVE | CVE-2021-36046 |
| CVE | CVE-2021-36047 |
| CVE | CVE-2021-36048 |

| | |
|------|----------------|
| CVE | CVE-2021-36050 |
| CVE | CVE-2021-36051 |
| CVE | CVE-2021-36052 |
| CVE | CVE-2021-36053 |
| CVE | CVE-2021-36054 |
| CVE | CVE-2021-36055 |
| CVE | CVE-2021-36056 |
| CVE | CVE-2021-36058 |
| CVE | CVE-2021-36064 |
| CVE | CVE-2021-39847 |
| CVE | CVE-2021-40716 |
| CVE | CVE-2021-40732 |
| CVE | CVE-2021-42528 |
| CVE | CVE-2021-42529 |
| CVE | CVE-2021-42530 |
| CVE | CVE-2021-42531 |
| CVE | CVE-2021-42532 |
| XREF | USN:5483-1 |

Plugin Information

Published: 2022/06/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libexpat1_2.5.1-1build1
- Fixed package : libexpat1_2.5.1-1ubuntu0.1

167852 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerabilities (USN-5638-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5638-2 advisory.

USN-5638-1 fixed a vulnerability in Expat. This update provides the corresponding updates for Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

It was discovered that Expat incorrectly handled memory in out-of-memory situations. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code.

This issue only affected Ubuntu 18.04 LTS. (CVE-2022-43680)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5638-2>

Solution

Update the affected expat, libexpat1 and / or libexpat1-dev 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)

References

| | |
|------|----------------|
| CVE | CVE-2022-40674 |
| CVE | CVE-2022-43680 |
| XREF | USN:5638-2 |

Plugin Information

Published: 2022/11/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.5

168146 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeRDP vulnerabilities (USN-5734-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5734-1 advisory.

It was discovered that FreeRDP incorrectly handled certain data lengths. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS.
(CVE-2022-39282, CVE-2022-39283)

It was discovered that FreeRDP incorrectly handled certain data lengths. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2022-39316, CVE-2022-39317, CVE-2022-39318, CVE-2022-39319, CVE-2022-39320)

It was discovered that FreeRDP incorrectly handled certain path checks. A malicious server could use this issue to cause FreeRDP clients to read files outside of the shared directory. (CVE-2022-39347)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5734-1>

Solution

Update the affected 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:H/I:N/A:N)

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-39282 |
| CVE | CVE-2022-39283 |
| CVE | CVE-2022-39316 |
| CVE | CVE-2022-39317 |
| CVE | CVE-2022-39318 |
| CVE | CVE-2022-39319 |
| CVE | CVE-2022-39320 |
| CVE | CVE-2022-39347 |
| XREF | USN:5734-1 |

Plugin Information

Published: 2022/11/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.4
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.4
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.4

163305 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeType vulnerabilities (USN-5528-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5528-1 advisory.

It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5528-1>

Solution

Update the affected 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-2022-27404 |
| CVE | CVE-2022-27405 |
| CVE | CVE-2022-27406 |
| CVE | CVE-2022-31782 |

XREF

USN:5528-1

Plugin Information

Published: 2022/07/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libfreetype6_2.10.1-2
- Fixed package : libfreetype6_2.10.1-2ubuntu0.2

163872 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuTLS vulnerabilities (USN-5550-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5550-1 advisory.

It was discovered that GnuTLS incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2021-4209)

It was discovered that GnuTLS incorrectly handled the verification of certain pkcs7 signatures. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-2509)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5550-1>

Solution

Update the affected 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 |
| XREF | USN:5550-1 |

Plugin Information

Published: 2022/08/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2

- Fixed package : libgnutls30_3.6.13-2ubuntu1.7

161922 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NTFS-3G vulnerabilities (USN-5463-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5463-1 advisory.

It was discovered that NTFS-3G incorrectly handled the ntfsck tool. If a user or automated system were tricked into using ntfsck on a specially crafted disk image, a remote attacker could possibly use this issue to execute arbitrary code. (CVE-2021-46790)

Roman Fiedler discovered that NTFS-3G incorrectly handled certain return codes. A local attacker could possibly use this issue to intercept protocol traffic between FUSE and the kernel. (CVE-2022-30783)

It was discovered that NTFS-3G incorrectly handled certain NTFS disk images. If a user or automated system were tricked into mounting a specially crafted disk image, a remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-30784, CVE-2022-30786, CVE-2022-30788, CVE-2022-30789)

Roman Fiedler discovered that NTFS-3G incorrectly handled certain file handles. A local attacker could possibly use this issue to read and write arbitrary memory. (CVE-2022-30785, CVE-2022-30787)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5463-1>

Solution

Update the affected 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

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-2021-46790 |
| CVE | CVE-2022-30783 |
| CVE | CVE-2022-30784 |
| CVE | CVE-2022-30785 |
| CVE | CVE-2022-30786 |
| CVE | CVE-2022-30787 |
| CVE | CVE-2022-30788 |
| CVE | CVE-2022-30789 |
| XREF | USN:5463-1 |

Plugin Information

Published: 2022/06/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1
- Fixed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1.2

- Installed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1
- Fixed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1.2

163680 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Net-SNMP vulnerabilities (USN-5543-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5543-1 advisory.

Yu Zhang and Nanyu Zhong discovered that Net-SNMP incorrectly handled memory operations when processing certain requests. A remote attacker could use this issue to cause Net-SNMP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5543-1>

Solution

Update the affected 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 (CVSS:2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS:2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2022-24805 |
| CVE | CVE-2022-24806 |
| CVE | CVE-2022-24807 |
| CVE | CVE-2022-24808 |
| CVE | CVE-2022-24809 |
| CVE | CVE-2022-24810 |
| XREF | USN:5543-1 |
| XREF | IAVA:2022-A-0305 |

Plugin Information

Published: 2022/08/01, Modified: 2025/02/11

Plugin Output

tcp/0

- Installed package : libsnmp-base_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp-base_5.8+dfsg-2ubuntu2.4

- Installed package : libsnmp35_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp35_5.8+dfsg-2ubuntu2.6

169711 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Net-SNMP vulnerabilities (USN-5795-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5795-1 advisory.

It was discovered that Net-SNMP incorrectly handled certain requests. A remote attacker could possibly use these issues to cause Net-SNMP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5795-1>

Solution

Update the affected 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-2022-44792 |
| CVE | CVE-2022-44793 |
| XREF | USN:5795-1 |

Plugin Information

Published: 2023/01/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsnmp-base_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp-base_5.8+dfsg-2ubuntu2.6

- Installed package : libsnmp35_5.8+dfsg-2ubuntu2.2
- Fixed package : libsnmp35_5.8+dfsg-2ubuntu2.6

161250 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-5424-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5424-1 advisory.

It was discovered that OpenLDAP incorrectly handled certain SQL statements within LDAP queries in the experimental back-sql backend. A remote attacker could possibly use this issue to perform an SQL injection attack and alter the database.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5424-1>

Solution

Update the affected 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-2022-29155
XREF-USN:5424-1

Plugin Information

Published: 2022/05/17, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.9

- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.9
```

167061 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : SQLite vulnerability (USN-5716-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5716-1 advisory.

It was discovered that SQLite incorrectly handled certain long string arguments. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5716-1>

Solution

Update the affected 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-2022-35737 |
| XREF | USN:5716-1 |
| XREF | IAVA:2022-A-0382-S |

Plugin Information

Published: 2022/11/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.5
```

174460 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6026-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6026-1 advisory.

It was discovered that Vim was incorrectly processing Vim buffers. An

attacker could possibly use this issue to perform illegal memory access and expose sensitive information.

This issue only affected Ubuntu 20.04 LTS. (CVE-2021-4166)

It was discovered that Vim was using freed memory when dealing with regular expressions inside a visual selection. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-4192)

It was discovered that Vim was incorrectly handling virtual column position operations, which could result in an out-of-bounds read. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-4193)

It was discovered that Vim was not properly performing bounds checks when updating windows present on a screen, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0213)

It was discovered that Vim was incorrectly performing read and write operations when in visual block mode, going beyond the end of a line and causing a heap buffer overflow. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-0261, CVE-2022-0318)

It was discovered that Vim was incorrectly handling window exchanging operations when in Visual mode, which could result in an out-of-bounds read. An attacker could possibly use this issue to expose sensitive information. (CVE-2022-0319)

It was discovered that Vim was incorrectly handling recursion when parsing conditional expressions. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0351)

It was discovered that Vim was not properly handling memory allocation when processing data in Ex mode, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0359)

It was discovered that Vim was not properly performing bounds checks when executing line operations in Visual mode, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-0361, CVE-2022-0368)

It was discovered that Vim was not properly handling loop conditions when looking for spell suggestions, which could result in a stack buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0408)

It was discovered that Vim was incorrectly handling memory access when executing buffer operations, which could result in the usage of freed memory. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-0443)

It was discovered that Vim was incorrectly processing Vim buffers. An attacker could possibly use this issue to perform illegal memory access and expose sensitive information. (CVE-2022-0554)

It was discovered that Vim was not properly performing bounds checks for column numbers when replacing tabs with spaces or spaces with tabs, which could cause a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0572)

It was discovered that Vim was incorrectly processing Vim buffers. An attacker could possibly use this issue to perform illegal memory access and expose sensitive information. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-0629)

It was discovered that Vim was not properly performing validation of data that contained special multi- byte characters, which could cause an out-of-bounds read. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0685)

It was discovered that Vim was incorrectly processing data used to define indentation in a file, which could cause a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0714)

It was discovered that Vim was incorrectly processing certain regular expression patterns and strings, which could cause an out-of-bounds read. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0729)

It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution. (CVE-2022-2207)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6026-1>

Solution

Update the affected 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-2021-4166 |
| CVE | CVE-2021-4192 |

| | |
|------|---------------|
| CVE | CVE-2021-4193 |
| CVE | CVE-2022-0213 |
| CVE | CVE-2022-0261 |
| CVE | CVE-2022-0318 |
| 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-2022-0443 |
| CVE | CVE-2022-0554 |
| CVE | CVE-2022-0572 |
| CVE | CVE-2022-0629 |
| CVE | CVE-2022-0685 |
| CVE | CVE-2022-0714 |
| CVE | CVE-2022-0729 |
| CVE | CVE-2022-2207 |
| XREF | USN:6026-1 |

Plugin Information

Published: 2023/04/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.14
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.14
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.14

168724 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerabilities (USN-5778-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5778-1 advisory.

Jan-Niklas Sohn discovered that X.Org X Server extensions contained multiple security issues. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5778-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-4283 |
| CVE | CVE-2022-46340 |
| CVE | CVE-2022-46341 |
| CVE | CVE-2022-46342 |
| CVE | CVE-2022-46343 |
| CVE | CVE-2022-46344 |
| XREF | USN:5778-1 |

Plugin Information

Published: 2022/12/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.5
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.5
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.5
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.5
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.5

162554 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5495-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5495-1 advisory.

Harry Sintonen discovered that curl incorrectly handled certain cookies. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 21.10, and Ubuntu 22.04 LTS.

(CVE-2022-32205)

Harry Sintonen discovered that curl incorrectly handled certain HTTP compressions. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-32206)

Harry Sintonen incorrectly handled certain file permissions. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 21.10, and Ubuntu 22.04 LTS.

(CVE-2022-32207)

Harry Sintonen discovered that curl incorrectly handled certain FTP-KRB messages. An attacker could possibly use this to perform a machine-in-the-middle attack. (CVE-2022-32208)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5495-1>

Solution

Update the affected 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)

STIG Severity

II

References

| | |
|------|--------------------|
| CVE | CVE-2022-32205 |
| CVE | CVE-2022-32206 |
| CVE | CVE-2022-32207 |
| CVE | CVE-2022-32208 |
| XREF | USN:5495-1 |
| XREF | IAVA:2022-A-0255-S |

Plugin Information

Published: 2022/06/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.12
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.12

169585 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5788-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5788-1 advisory.

Hiroki Kurosawa discovered that curl incorrectly handled HSTS support when certain hostnames included IDN characters. A remote attacker could possibly use this issue to cause curl to use unencrypted connections.

This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-43551)

It was discovered that curl incorrectly handled denials when using HTTP proxies. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-43552)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5788-1>

Solution

Update the affected 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: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:I/N/A:N)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2022-43551 |
| CVE | CVE-2022-43552 |
| XREF | USN:5788-1 |
| XREF | IAVA:2023-A-0008-S |

Plugin Information

Published: 2023/01/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.15
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.15

171942 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5891-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5891-1 advisory.

Harry Sintonen discovered that curl incorrectly handled HSTS support when multiple URLs are requested serially. A remote attacker could possibly use this issue to cause curl to use unencrypted connections.

This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-23914)

Harry Sintonen discovered that curl incorrectly handled HSTS support when multiple URLs are requested in parallel. A remote attacker could possibly use this issue to cause curl to use unencrypted connections.

This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-23915)

Patrick Monnerat discovered that curl incorrectly handled memory when processing requests with multi- header compression. A remote attacker could possibly use this issue to cause curl to consume resources, leading to a denial of service. (CVE-2023-23916)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5891-1>

Solution

Update the affected 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:H/A:N)

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:I/C:A:N)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-23914 |
| CVE | CVE-2023-23915 |
| CVE | CVE-2023-23916 |
| XREF | USN:5891-1 |
| XREF | IAVA:2023-A-0008-S |
| XREF | IAVA:2023-A-0108-S |

Plugin Information

Published: 2023/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.16

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.16

161613 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : dpkg vulnerability (USN-5446-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5446-1 advisory.

Max Justicz discovered that dpkg incorrectly handled unpacking certain source packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could modify files outside the target unpack directory, leading to a denial of service or potentially gaining access to the system.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5446-1>

Solution

Update the affected 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

8.5 (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 |
| XREF | USN:5446-1 |

Plugin Information

Published: 2022/05/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : dpkg_1.19.7ubuntu3
- Fixed package : dpkg_1.19.7ubuntu3.2
- Installed package : dpkg-dev_1.19.7ubuntu3
- Fixed package : dpkg-dev_1.19.7ubuntu3.2
- Installed package : libdpkg-perl_1.19.7ubuntu3
- Fixed package : libdpkg-perl_1.19.7ubuntu3.2

170110 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : libXpm vulnerabilities (USN-5807-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5807-1 advisory.

Martin Ettl discovered that libXpm incorrectly handled certain XPM files. If a user or automated system were tricked into opening a specially crafted XPM file, a remote attacker could possibly use this issue to cause libXpm to stop responding, resulting in a denial of service. (CVE-2022-44617)

Marco Ivaldi discovered that libXpm incorrectly handled certain XPM files. If a user or automated system were tricked into opening a specially crafted XPM file, a remote attacker could possibly use this issue to cause libXpm to stop responding, resulting in a denial of service. (CVE-2022-46285)

Alan Coopersmith discovered that libXpm incorrectly handled calling external helper binaries. If libXpm was being used by a setuid binary, a local attacker could possibly use this issue to escalate privileges.

(CVE-2022-4883)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5807-1>

Solution

Update the affected libxpm-dev, libxpm4 and / or xpmutils 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 |
| XREF | USN:5807-1 |

Plugin Information

Published: 2023/01/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libxpm4_1:3.5.12-1
- Fixed package : libxpm4_1:3.5.12-1ubuntu0.20.04.1

172126 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : rsync vulnerabilities (USN-5921-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5921-1 advisory.

Koen van Hove discovered that the rsync client incorrectly validated filenames returned by servers. If a user or automated system were tricked into connecting to a malicious server, a remote attacker could use this issue to write arbitrary files, and possibly escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5921-1>

Solution

Update the affected rsync package.

Risk Factor

High

CVSS v3.0 Base Score

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

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:N/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-29154 |
| XREF | USN:5921-1 |

Plugin Information

Published: 2023/03/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : rsync_3.1.3-8
- Fixed package : rsync_3.1.3-8ubuntu0.5

150940 - Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-4994-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4994-1 advisory.

Marc Stern discovered that the Apache mod_proxy_http module incorrectly handled certain requests. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. (CVE-2020-13950)

Antonio Morales discovered that the Apache mod_auth_digest module incorrectly handled certain Digest nonces. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. (CVE-2020-35452)

Antonio Morales discovered that the Apache mod_session module incorrectly handled certain Cookie headers.

A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. (CVE-2021-26690)

Christophe Jaillet discovered that the Apache mod_session module incorrectly handled certain SessionHeader values. A remote attacker could use this issue to cause Apache to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-26691)

Christoph Anton Mitterer discovered that the new MergeSlashes configuration option resulted in unexpected behaviour in certain situations. (CVE-2021-30641)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4994-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-13950 |
| CVE | CVE-2020-35452 |
| CVE | CVE-2021-26690 |
| CVE | CVE-2021-26691 |
| CVE | CVE-2021-30641 |
| XREF | USN:4994-1 |
| XREF | IAVA:2021-A-0259-S |

Plugin Information

Published: 2021/06/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.3
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.3
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.3
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.3

153768 - Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-5090-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5090-1 advisory.

James Kettle discovered that the Apache HTTP Server HTTP/2 module incorrectly handled certain crafted methods. A remote attacker could possibly use this issue to perform request splitting or cache poisoning attacks. (CVE-2021-33193)

It was discovered that the Apache HTTP Server incorrectly handled certain malformed requests. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service.

(CVE-2021-34798)

Li Zhi Xin discovered that the Apache mod_proxy_uwsgi module incorrectly handled certain request uri- paths. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-36160)

It was discovered that the Apache HTTP Server incorrectly handled escaping quotes. If the server was configured with third-party modules, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-39275)

It was discovered that the Apache mod_proxy module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to forward requests to arbitrary origin servers. (CVE-2021-40438)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5090-1>

Solution

Update the affected 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

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-2021-33193 |
| CVE | CVE-2021-34798 |
| CVE | CVE-2021-36160 |
| CVE | CVE-2021-39275 |
| CVE | CVE-2021-40438 |
| XREF | USN:5090-1 |
| XREF | IAVA:2021-A-0440-S |
| XREF | CISA-KNOWN-EXPLOITED:2021/12/15 |

Plugin Information

Published: 2021/09/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.5
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.5
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.5
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.5

156544 - Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-5212-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5212-1 advisory.

It was discovered that the Apache HTTP Server incorrectly handled certain forward proxy requests. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly perform a Server Side Request Forgery attack. (CVE-2021-44224)

It was discovered that the Apache HTTP Server Lua module incorrectly handled memory in the multipart parser. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-44790)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5212-1>

Solution

Update the affected 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/R:L/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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-44224 |
| CVE | CVE-2021-44790 |
| XREF | USN:5212-1 |
| XREF | IAVA:2021-A-0604-S |

Plugin Information

Published: 2022/01/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.9
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.9
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.9
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.9

159024 - Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-5333-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5333-1 advisory.

Chamal De Silva discovered that the Apache HTTP Server mod_lua module incorrectly handled certain crafted request bodies. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2022-22719)

James Kettle discovered that the Apache HTTP Server incorrectly closed inbound connection when certain errors are encountered. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2022-22720)

It was discovered that the Apache HTTP Server incorrectly handled large LimitXMLRequestBody settings on certain platforms. In certain configurations, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22721)

Ronald Crane discovered that the Apache HTTP Server mod_sed module incorrectly handled memory. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-23943)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5333-1>

Solution

Update the affected 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

8.5 (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-2022-22719 |
| CVE | CVE-2022-22720 |
| CVE | CVE-2022-22721 |
| CVE | CVE-2022-23943 |
| XREF | USN:5333-1 |
| XREF | IAVA:2022-A-0124-S |

Plugin Information

Published: 2022/03/17, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.10
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.10
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.10
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.10

150809 - Ubuntu 18.04 LTS / 20.04 LTS : BlueZ vulnerabilities (USN-4989-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4989-1 advisory.

It was discovered that BlueZ incorrectly checked certain permissions when pairing. A local attacker could possibly use this issue to impersonate devices. (CVE-2020-26558)

Jay LV discovered that BlueZ incorrectly handled redundant disconnect MGMT events. A local attacker could use this issue to cause BlueZ to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-27153)

Ziming Zhang discovered that BlueZ incorrectly handled certain array indexes. A local attacker could use this issue to cause BlueZ to crash, resulting in a denial of service, or possibly obtain sensitive information. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2021-3588)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4989-1>

Solution

Update the affected packages.

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

7.7 (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-2020-26558 |
| CVE | CVE-2020-27153 |
| CVE | CVE-2021-3588 |
| XREF | USN:4989-1 |

Plugin Information

Published: 2021/06/16, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.2
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.2
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.2
- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.2

160853 - Ubuntu 18.04 LTS / 20.04 LTS : DBus vulnerability (USN-5244-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5244-2 advisory.

USN-5244-1 fixed a vulnerability in DBus. This update provides the corresponding update for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5244-2>

Solution

Update the affected 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-2020-35512 |
| XREF | USN:5244-2 |

Plugin Information

Published: 2022/05/10, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : dbus_1.12.16-2ubuntu2.1
- Fixed package : dbus_1.12.16-2ubuntu2.2
- Installed package : dbus-user-session_1.12.16-2ubuntu2.1
- Fixed package : dbus-user-session_1.12.16-2ubuntu2.2
- Installed package : dbus-x11_1.12.16-2ubuntu2.1
- Fixed package : dbus-x11_1.12.16-2ubuntu2.2
- Installed package : libdbus-1-3_1.12.16-2ubuntu2.1
- Fixed package : libdbus-1-3_1.12.16-2ubuntu2.2

141863 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4599-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4599-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the prompt for opening an external application, obtain sensitive information, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4599-1>

Solution

Update the affected 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/R:L/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-2020-15254 |
| CVE | CVE-2020-15680 |
| CVE | CVE-2020-15681 |
| CVE | CVE-2020-15682 |
| CVE | CVE-2020-15683 |
| CVE | CVE-2020-15684 |
| CVE | CVE-2020-15969 |
| XREF | USN:4599-1 |

Plugin Information

Published: 2020/10/24, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_82.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_82.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_82.0+build2-0ubuntu0.20.04.1

143121 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4637-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4637-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across origins, bypass security restrictions, conduct phishing attacks, conduct cross-site scripting (XSS) attacks, bypass Content Security Policy (CSP) restrictions, conduct DNS rebinding attacks, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4637-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2020-16012 |
| CVE | CVE-2020-26951 |
| CVE | CVE-2020-26952 |

| | |
|------|----------------|
| CVE | CVE-2020-26953 |
| CVE | CVE-2020-26956 |
| CVE | CVE-2020-26958 |
| CVE | CVE-2020-26959 |
| CVE | CVE-2020-26960 |
| CVE | CVE-2020-26961 |
| CVE | CVE-2020-26962 |
| CVE | CVE-2020-26963 |
| CVE | CVE-2020-26965 |
| CVE | CVE-2020-26967 |
| CVE | CVE-2020-26968 |
| CVE | CVE-2020-26969 |
| XREF | USN:4637-1 |

Plugin Information

Published: 2020/11/19, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_83.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_83.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_83.0+build2-0ubuntu0.20.04.1
```

154883 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5131-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5131-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, spoof the browser UI, confuse the user, conduct phishing attacks, or execute arbitrary code. (CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509)

It was discovered that the 'Copy Image Link' context menu action would copy the final image URL after redirects. If a user were tricked into copying and pasting a link for an embedded image that triggered authentication flows back to the page, an attacker could potentially exploit this to steal authentication tokens.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5131-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.7 (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-2021-38503 |
| CVE | CVE-2021-38504 |
| CVE | CVE-2021-38506 |
| CVE | CVE-2021-38507 |
| CVE | CVE-2021-38508 |
| CVE | CVE-2021-38509 |
| XREF | USN:5131-1 |
| XREF | IAVA:2021-A-0527-S |

Plugin Information

Published: 2021/11/03, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_94.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_94.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_94.0+build3-0ubuntu0.20.04.1

159589 - Ubuntu 18.04 LTS / 20.04 LTS : FriBidi vulnerabilities (USN-5366-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5366-1 advisory.

It was discovered that FriBidi incorrectly handled processing of input strings resulting in memory corruption. An attacker could use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25308)

It was discovered that FriBidi incorrectly validated input data to its CapRTL unicode encoder, resulting in memory corruption. An attacker could use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25309)

It was discovered that FriBidi incorrectly handled empty input when removing marks from unicode strings, resulting in a crash. An attacker could use this to cause FriBidi to crash, resulting in a denial of service, or potentially

execute arbitrary code. (CVE-2022-25310)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5366-1>

Solution

Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 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-2022-25308 |
| CVE | CVE-2022-25309 |
| CVE | CVE-2022-25310 |
| XREF | USN:5366-1 |

Plugin Information

Published: 2022/04/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libfribidi0_1.0.8-2
- Fixed package : libfribidi0_1.0.8-2ubuntu0.1

158502 - Ubuntu 18.04 LTS / 20.04 LTS : GNU C Library vulnerabilities (USN-5310-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5310-1 advisory.

Jan Engelhardt, Tavis Ormandy, and others discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could possibly use this issue to cause the GNU C Library to hang or crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2016-10228, CVE-2019-25013, CVE-2020-27618, CVE-2020-29562, CVE-2021-3326)

Jason Royes and Samuel Dytrych discovered that the GNU C Library incorrectly handled signed comparisons on ARMv7 targets. A remote attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-6096)

It was discovered that the GNU C Library nscd daemon incorrectly handled certain netgroup lookups. An attacker could possibly use this issue to cause the GNU C Library to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-27645)

It was discovered that the GNU C Library wordexp function incorrectly handled certain patterns. An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly obtain sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-35942)

It was discovered that the GNU C Library realpath function incorrectly handled return values. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 21.10. (CVE-2021-3998)

It was discovered that the GNU C library getcwd function incorrectly handled buffers. An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-3999)

It was discovered that the GNU C Library sunrpc module incorrectly handled buffer lengths. An attacker could possibly use this issue to cause the GNU C Library to crash, resulting in a denial of service. (CVE-2022-23218, CVE-2022-23219)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5310-1>

Solution

Update the affected 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-2019-25013 |
| CVE | CVE-2020-6096 |
| CVE | CVE-2020-27618 |
| CVE | CVE-2020-29562 |
| CVE | CVE-2021-3326 |
| CVE | CVE-2021-3998 |
| CVE | CVE-2021-3999 |
| CVE | CVE-2021-27645 |
| CVE | CVE-2021-35942 |
| CVE | CVE-2022-23218 |
| CVE | CVE-2022-23219 |
| XREF | USN:5310-1 |

Plugin Information

Published: 2022/03/01, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.7
- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.7
- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.7
- Installed package : libc6-dev_2.31-0ubuntu9
- Fixed package : libc6-dev_2.31-0ubuntu9.7
- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.7

159711 - Ubuntu 18.04 LTS / 20.04 LTS : Gzip vulnerability (USN-5378-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5378-1 advisory.

Cleemy Desu Wayo discovered that Gzip incorrectly handled certain filenames. If a user or automated system were tricked into performing zgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5378-1>

Solution

Update the affected gzip and / or gzip-win32 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: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 | USN:5378-1 |
| XREF | IAVA:2024-A-0327 |

Plugin Information

Published: 2022/04/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gzip_1.10-0ubuntu4
- Fixed package : gzip_1.10-0ubuntu4.1

149988 - Ubuntu 18.04 LTS / 20.04 LTS : LZ4 vulnerability (USN-4968-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4968-1 advisory.

It was discovered that LZ4 incorrectly handled certain memory operations. If a user or automated system were tricked into uncompressing a specially- crafted LZ4 file, a remote attacker could use this issue to cause LZ4 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4968-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3520 |
| XREF | USN:4968-1 |

Plugin Information

Published: 2021/05/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : liblzip4-1_1.9.2-2
- Fixed package : liblzip4-1_1.9.2-2ubuntu0.20.04.1
- Installed package : lz4_1.9.2-2
- Fixed package : lz4_1.9.2-2ubuntu0.20.04.1

174410 - Ubuntu 18.04 LTS / 20.04 LTS : LibreOffice vulnerability (USN-6023-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6023-1 advisory.

It was discovered that LibreOffice may be configured to add an empty entry to the Java class path. This may lead to run arbitrary Java code from the current directory.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6023-1>

Solution

Update the affected 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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-38745 |
| XREF | USN:6023-1 |

Plugin Information

Published: 2023/04/17, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.7

- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.7

- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.7
```

- Installed package : libuno-purpenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.7
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.7
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.7
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.7
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.7
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.7

145234 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel update (USN-4689-4)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4689-4 advisory.

USN-4689-3 fixed vulnerabilities in the NVIDIA server graphics drivers. This update provides the corresponding updates for the NVIDIA Linux DKMS kernel modules.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4689-4>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/U: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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2021-1052 |
| CVE | CVE-2021-1053 |
| XREF | USN:4689-4 |

Plugin Information

Published: 2021/01/21, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-64-generic for this advisory.

140181 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4483-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4483-1 advisory.

Chuhong Yuan discovered that go7007 USB audio device driver in the Linux kernel did not properly deallocate memory in some failure conditions. A physically proximate attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-20810)

Fan Yang discovered that the mremap implementation in the Linux kernel did not properly handle DAX Huge Pages. A local attacker with access to DAX storage could use this to gain administrative privileges.

(CVE-2020-10757)

It was discovered that the Linux kernel did not correctly apply Speculative Store Bypass Disable (SSBD) mitigations in certain situations. A local attacker could possibly use this to expose sensitive information. (CVE-2020-10766)

It was discovered that the Linux kernel did not correctly apply Indirect Branch Predictor Barrier (IBPB) mitigations in certain situations. A local attacker could possibly use this to expose sensitive information. (CVE-2020-10767)

It was discovered that the Linux kernel could incorrectly enable Indirect Branch Speculation after it has been disabled for a process via a prctl() call. A local attacker could possibly use this to expose sensitive information. (CVE-2020-10768)

Luca Bruno discovered that the zram module in the Linux kernel did not properly restrict unprivileged users from accessing the hot_add sysfs file. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2020-10781)

It was discovered that the XFS file system implementation in the Linux kernel did not properly validate meta data in some circumstances. An attacker could use this to construct a malicious XFS image that, when mounted, could cause a denial of service. (CVE-2020-12655)

It was discovered that the bcache subsystem in the Linux kernel did not properly release a lock in some error conditions. A local attacker could possibly use this to cause a denial of service. (CVE-2020-12771)

It was discovered that the Virtual Terminal keyboard driver in the Linux kernel contained an integer overflow. A local attacker could possibly use this to have an unspecified impact. (CVE-2020-13974)

It was discovered that the cgroup v2 subsystem in the Linux kernel did not properly perform reference counting in some situations, leading to a NULL pointer dereference. A local attacker could use this to cause a denial of service or possibly gain administrative privileges. (CVE-2020-14356)

Kyungtae Kim discovered that the USB testing driver in the Linux kernel did not properly deallocate memory on disconnect events. A physically proximate attacker could use this to cause a denial of service (memory exhaustion). (CVE-2020-15393)

It was discovered that the NFS server implementation in the Linux kernel did not properly honor umask settings when setting permissions while creating file system objects if the underlying file system did not support ACLs. An attacker could possibly use this to expose sensitive information or violate system integrity. (CVE-2020-24394)

It was discovered that the Kerberos SUNRPC GSS implementation in the Linux kernel did not properly deallocate memory on module unload. A local privileged attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2020-12656)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4483-1>

Solution

Update the affected kernel package.

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

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2019-20810 |
| CVE | CVE-2020-10757 |
| CVE | CVE-2020-10766 |
| CVE | CVE-2020-10767 |
| CVE | CVE-2020-10768 |
| CVE | CVE-2020-10781 |
| CVE | CVE-2020-12655 |
| CVE | CVE-2020-12656 |
| CVE | CVE-2020-12771 |
| CVE | CVE-2020-13974 |
| CVE | CVE-2020-14356 |
| CVE | CVE-2020-15393 |
| CVE | CVE-2020-24394 |
| XREF | USN:4483-1 |

Plugin Information

Published: 2020/09/02, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-45-generic for this advisory.

143431 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4658-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4658-1 advisory.

It was discovered that a race condition existed in the binder IPC implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-0423)

Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen discovered that legacy pairing and secure- connections pairing authentication in the Bluetooth protocol could allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. A physically proximate attacker could use this to impersonate a previously paired Bluetooth device. (CVE-2020-10135)

It was discovered that a race condition existed in the perf subsystem of the Linux kernel, leading to a use-after-free vulnerability. An attacker with access to the perf subsystem could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-14351)

It was discovered that the frame buffer implementation in the Linux kernel did not properly handle some edge cases in software scrollback. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-14390)

It was discovered that the netfilter connection tracker for netlink in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-25211)

It was discovered that the Rados block device (rbd) driver in the Linux kernel did not properly perform privilege checks for access to rbd devices in some situations. A local attacker could use this to map or unmap rbd block devices. (CVE-2020-25284)

It was discovered that the HDLC PPP implementation in the Linux kernel did not properly validate input in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-25643)

It was discovered that the GENEVE tunnel implementation in the Linux kernel when combined with IPsec did not properly select IP routes in some situations. An attacker could use this to expose sensitive information (unencrypted network traffic). (CVE-2020-25645)

Keyu Man discovered that the ICMP global rate limiter in the Linux kernel could be used to assist in scanning open UDP ports. A remote attacker could use to facilitate attacks on UDP based services that depend on source port randomization. (CVE-2020-25705)

It was discovered that the framebuffer implementation in the Linux kernel did not properly perform range checks in certain situations. A local attacker could use

this to expose sensitive information (kernel memory). (CVE-2020-28915)

It was discovered that Power 9 processors could be coerced to expose information from the L1 cache in certain situations. A local attacker could use this to expose sensitive information. (CVE-2020-4788)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4658-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------------|
| CVE | CVE-2020-0423 |
| CVE | CVE-2020-4788 |
| CVE | CVE-2020-10135 |
| CVE | CVE-2020-14351 |
| CVE | CVE-2020-14390 |
| CVE | CVE-2020-25211 |
| CVE | CVE-2020-25284 |
| CVE | CVE-2020-25643 |
| CVE | CVE-2020-25645 |
| CVE | CVE-2020-25705 |
| CVE | CVE-2020-28915 |
| XREF | USN:4658-1 |
| XREF | CEA-ID:CEA-2020-0138 |

Plugin Information

Published: 2020/12/02, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-56-generic for this advisory.

144750 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4679-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4679-1 advisory.

It was discovered that the console keyboard driver in the Linux kernel contained a race condition. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-25656)

Minh Yuan discovered that the tty driver in the Linux kernel contained race conditions when handling fonts. A local attacker could possibly use this to expose sensitive information (kernel memory).

(CVE-2020-25668)

Kiyin () discovered that the perf subsystem in the Linux kernel did not properly deallocate memory in some situations. A privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2020-25704)

Jinoh Kang discovered that the Xen event channel infrastructure in the Linux kernel contained a race condition. An attacker in guest could possibly use this to cause a denial of service (dom0 crash).
(CVE-2020-27675)

Daniel Axtens discovered that PowerPC RTAS implementation in the Linux kernel did not properly restrict memory accesses in some situations. A privileged local attacker could use this to arbitrarily modify kernel memory, potentially bypassing kernel lockdown restrictions. (CVE-2020-27777)

Minh Yuan discovered that the framebuffer console driver in the Linux kernel did not properly handle fonts in some conditions. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2020-28974)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4679-1>

Solution

Update the affected kernel package.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-25656 |
| CVE | CVE-2020-25668 |
| CVE | CVE-2020-25704 |
| CVE | CVE-2020-27675 |
| CVE | CVE-2020-27777 |
| CVE | CVE-2020-28974 |
| XREF | USN:4679-1 |

Plugin Information

Published: 2021/01/06, Modified: 2024/08/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-59-generic for this advisory.

144869 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4689-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4689-2 advisory.

USN-4689-1 fixed vulnerabilities in the NVIDIA graphics drivers. This update provides the corresponding updates for the NVIDIA Linux DKMS kernel modules.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4689-2>

Solution

Update the affected kernel package.

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

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-2021-1052 |
| CVE | CVE-2021-1053 |
| CVE | CVE-2021-1056 |
| XREF | USN:4689-2 |

Plugin Information

Published: 2021/01/12, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-60-generic for this advisory.

148009 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4750-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4750-1 advisory.

Bodong Zhao discovered a use-after-free in the Sun keyboard driver implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

(CVE-2020-25669)

It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service (system crash).

(CVE-2020-27815)

Shisong Qin and Bodong Zhao discovered that Speakup screen reader driver in the Linux kernel did not correctly handle setting line discipline in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-27830, CVE-2020-28941)

It was discovered that an information leak existed in the syscall implementation in the Linux kernel on 32 bit systems. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2020-28588)

Michael Kurth and Paweł Wieczorkiewicz discovered that the Xen event processing backend in the Linux kernel did not properly limit the number of events queued. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2020-29568)

Olivier Benjamin and Paweł Wieczorkiewicz discovered a race condition the Xen paravirt block backend in the Linux kernel, leading to a use-after-free vulnerability. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2020-29569)

Jann Horn discovered that the tty subsystem of the Linux kernel did not use consistent locking in some situations, leading to a read-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2020-29660)

Jann Horn discovered a race condition in the tty subsystem of the Linux kernel in the locking for the TIOCSPGRP ioctl(), leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-29661)

It was discovered that the netfilter subsystem in the Linux kernel did not properly handle filter rules in some situations. A local attacker with the CAP_NET_ADMIN capability could use this to cause a denial of service. (CVE-2021-20177)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4750-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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-2020-25669 |
| CVE | CVE-2020-27815 |
| CVE | CVE-2020-27830 |
| CVE | CVE-2020-28588 |
| CVE | CVE-2020-28941 |
| CVE | CVE-2020-29568 |
| CVE | CVE-2020-29569 |
| CVE | CVE-2020-29660 |
| CVE | CVE-2020-29661 |
| CVE | CVE-2021-20177 |
| XREF | USN:4750-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-66-generic for this advisory.

148003 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4878-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4878-1 advisory.

It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad- hoc SSIDs. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-36158)

Ryota Shiga discovered that the sockopt BPF hooks in the Linux kernel could allow a user space program to probe for valid kernel addresses. A local attacker could use this to ease exploitation of another kernel vulnerability. (CVE-2021-20239)

It was discovered that the priority inheritance futex implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3347)

discovered that the NFS implementation in the Linux kernel did not properly prevent access outside of an NFS export that is a subdirectory of a file system. An attacker could possibly use this to bypass NFS access restrictions. (CVE-2021-3178)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4878-1>

Solution

Update the affected kernel package.

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

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-2020-36158 |
| CVE | CVE-2021-3178 |
| CVE | CVE-2021-3347 |
| CVE | CVE-2021-20239 |
| XREF | USN:4878-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-67-generic for this advisory.

148690 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4917-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4917-1 advisory.

It was discovered that the overlayfs implementation in the Linux kernel did not properly validate the application of file system capabilities with respect to user

namespaces. A local attacker could use this to gain elevated privileges. (CVE-2021-3493)

Vincent Dehors discovered that the shiftfs file system in the Ubuntu Linux kernel did not properly handle faults in copy_from_user() when passing through iocfts to an underlying file system. A local attacker could use this to cause a denial of service (memory exhaustion) or execute arbitrary code. (CVE-2021-3492)

Piotr Krysiuk discovered that the BPF JIT compiler for x86 in the Linux kernel did not properly validate computation of branch displacements in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-29154)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4917-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-3492 |
| CVE | CVE-2021-3493 |
| CVE | CVE-2021-29154 |
| XREF | USN:4917-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/11/10 |

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2021/04/16, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-72-generic for this advisory.

149416 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4945-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4945-1 advisory.

It was discovered that the Nouveau GPU driver in the Linux kernel did not properly handle error conditions in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-25639)

Jan Beulich discovered that the Xen netback backend in the Linux kernel did not properly handle certain error conditions under paravirtualization. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2021-28038)

It was discovered that the fastrpc driver in the Linux kernel did not prevent user space applications from sending kernel RPC messages. A local attacker could possibly use this to gain elevated privileges.
(CVE-2021-28375)

It was discovered that the Realtek RTL8188EU Wireless device driver in the Linux kernel did not properly validate ssid lengths in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2021-28660)

It was discovered that the USB/IP driver in the Linux kernel contained race conditions during the update of local and shared status. An attacker could use this to cause a denial of service (system crash).
(CVE-2021-29265)

It was discovered that a race condition existed in the netfilter subsystem of the Linux kernel when replacing tables. A local attacker could use this to cause a denial of service (system crash).
(CVE-2021-29650)

Arnd Bergmann discovered that the video4linux subsystem in the Linux kernel did not properly deallocate memory in some situations. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-30002)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4945-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-25639 |
| CVE | CVE-2021-28038 |
| CVE | CVE-2021-28375 |
| CVE | CVE-2021-28660 |
| CVE | CVE-2021-29265 |
| CVE | CVE-2021-29650 |
| CVE | CVE-2021-30002 |
| XREF | USN:4945-1 |

Plugin Information

Published: 2021/05/12, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-73-generic for this advisory.

150233 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4982-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4982-1 advisory.

Kiyin () discovered that the NFC LLCP protocol implementation in the Linux kernel contained a reference counting error. A local attacker could use this to cause a denial of service (system crash).

(CVE-2020-25670)

Kiyin () discovered that the NFC LLCP protocol implementation in the Linux kernel did not properly deallocate memory in certain error situations. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2020-25671, CVE-2020-25672)

Kiyin () discovered that the NFC LLCP protocol implementation in the Linux kernel did not properly handle error conditions in some situations, leading to an infinite loop. A local attacker could use this to cause a denial of service. (CVE-2020-25673)

It was discovered that the Xen paravirtualization backend in the Linux kernel did not properly deallocate memory in some situations. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-28688)

It was discovered that the fuse user space file system implementation in the Linux kernel did not properly handle bad inodes in some situations. A local attacker could possibly use this to cause a denial of service. (CVE-2021-28950)

Zygo Blaxell discovered that the btrfs file system implementation in the Linux kernel contained a race condition during certain cloning operations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-28964)

Vince Weaver discovered that the perf subsystem in the Linux kernel did not properly handle certain PEBS records properly for some Intel Haswell processors. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-28971)

It was discovered that the RPA PCI Hotplug driver implementation in the Linux kernel did not properly handle device name writes via sysfs, leading to a buffer overflow. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-28972)

It was discovered that the Freescale Gianfar Ethernet driver for the Linux kernel did not properly handle receive queue overrun when jumbo frames were enabled in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2021-29264)

It was discovered that the Qualcomm IPC router implementation in the Linux kernel did not properly initialize memory passed to user space. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-29647)

Dan Carpenter discovered that the block device manager (dm) implementation in the Linux kernel contained a buffer overflow in the ioctl for listing devices. A privileged local attacker could use this to cause a denial of service (system crash). (CVE-2021-31916)

discovered that the IEEE 1394 (Firewire) nosy packet sniffer driver in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3483)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4982-1>

Solution

Update the affected kernel package.

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

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-2020-25670 |
| CVE | CVE-2020-25671 |
| CVE | CVE-2020-25672 |
| CVE | CVE-2020-25673 |
| CVE | CVE-2021-3483 |
| CVE | CVE-2021-28688 |
| CVE | CVE-2021-28950 |
| CVE | CVE-2021-28964 |
| CVE | CVE-2021-28971 |
| CVE | CVE-2021-28972 |
| CVE | CVE-2021-29264 |
| CVE | CVE-2021-29647 |
| CVE | CVE-2021-31916 |
| XREF | USN:4982-1 |

Plugin Information

Published: 2021/06/03, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-74-generic for this advisory.

150957 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5000-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5000-1 advisory.

Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. (CVE-2021-3609)

Piotr Krysiuk discovered that the eBPF implementation in the Linux kernel did not properly enforce limits for pointer operations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33200)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation did not properly clear received fragments from memory in some situations. A physically proximate attacker could possibly use this issue to inject packets or expose sensitive information. (CVE-2020-24586)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation incorrectly handled encrypted fragments. A physically proximate attacker could possibly use this issue to decrypt fragments.
(CVE-2020-24587)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation incorrectly handled certain malformed frames. If a user were tricked into connecting to a malicious server, a physically proximate attacker could use this issue to inject packets. (CVE-2020-24588)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation incorrectly handled EAPOL frames from unauthenticated senders. A physically proximate attacker could inject malicious packets to cause a denial of service (system crash). (CVE-2020-26139)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation did not properly verify certain fragmented frames. A physically proximate attacker could possibly use this issue to inject or decrypt packets. (CVE-2020-26141)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation accepted plaintext fragments in certain situations. A physically proximate attacker could use this issue to inject packets.
(CVE-2020-26145)

Mathy Vanhoef discovered that the Linux kernels WiFi implementation could reassemble mixed encrypted and plaintext fragments. A physically proximate attacker could possibly use this issue to inject packets or exfiltrate selected fragments. (CVE-2020-26147)

Or Cohen discovered that the SCTP implementation in the Linux kernel contained a race condition in some situations, leading to a use-after-free condition. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-23133)

Or Cohen and Nadav Markus discovered a use-after-free vulnerability in the nfc implementation in the Linux kernel. A privileged local attacker could use this issue to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-23134)

Piotr Krysiuk discovered that the eBPF implementation in the Linux kernel did not properly prevent speculative loads in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-31829)

It was discovered that a race condition in the kernel Bluetooth subsystem could lead to use-after-free of slab objects. An attacker could use this issue to possibly execute arbitrary code. (CVE-2021-32399)

It was discovered that a use-after-free existed in the Bluetooth HCI driver of the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.
(CVE-2021-33034)

It was discovered that an out-of-bounds (OOB) memory access flaw existed in the f2fs module of the Linux kernel. A local attacker could use this issue to cause a denial of service (system crash). (CVE-2021-3506)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5000-1>

Solution

Update the affected kernel package.

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

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-2020-24586 |
| CVE | CVE-2020-24587 |
| CVE | CVE-2020-24588 |
| CVE | CVE-2020-26139 |
| CVE | CVE-2020-26141 |
| CVE | CVE-2020-26145 |
| CVE | CVE-2020-26147 |
| CVE | CVE-2021-3506 |
| CVE | CVE-2021-3609 |
| CVE | CVE-2021-23133 |
| CVE | CVE-2021-23134 |
| CVE | CVE-2021-31829 |
| CVE | CVE-2021-32399 |
| CVE | CVE-2021-33034 |
| CVE | CVE-2021-33200 |
| XREF | USN:5000-1 |

Plugin Information

Published: 2021/06/23, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-77-generic for this advisory.

153129 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5017-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5017-1 advisory.

It was discovered that the virtual file system implementation in the Linux kernel contained an unsigned to signed integer conversion error. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-33909)

It was discovered that the bluetooth subsystem in the Linux kernel did not properly perform access control. An authenticated attacker could possibly use this to expose sensitive information.
(CVE-2020-26558, CVE-2021-0129)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5017-1>

Solution

Update the affected kernel package.

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

7.5 (CVSS:3.0/E:H/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

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

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2020-26558 |
| CVE | CVE-2021-0129 |
| CVE | CVE-2021-33909 |
| XREF | USN:5017-1 |
| XREF | IAVA:2021-A-0350 |

Plugin Information

Published: 2021/09/08, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-80-generic for this advisory.

153178 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5071-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5071-1 advisory.

Maxim Levitsky and Paolo Bonzini discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel allowed a guest VM to disable restrictions on VMLOAD/VMSAVE in a nested guest. An attacker in a guest VM could use this to read or write portions of the host's physical memory.
(CVE-2021-3656)

Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling

AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. (CVE-2021-3653)

It was discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not ensure enough processing time was given to perform cleanups of large SEV VMs. A local attacker could use this to cause a denial of service (soft lockup). (CVE-2020-36311)

It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. An attacker who could start and control a VM could possibly use this to expose sensitive information or execute arbitrary code. (CVE-2021-22543)

Murray McAllister discovered that the joystick device interface in the Linux kernel did not properly validate data passed via an ioctl(). A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code on systems with a joystick device registered. (CVE-2021-3612)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5071-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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-2020-36311 |
| CVE | CVE-2021-3612 |
| CVE | CVE-2021-3653 |
| CVE | CVE-2021-3656 |
| CVE | CVE-2021-22543 |
| XREF | USN:5071-1 |

Plugin Information

Published: 2021/09/09, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-84-generic for this advisory.

153769 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5091-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5091-1 advisory.

Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack.

An attacker could use this to expose sensitive information. (CVE-2021-33624)

It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. (CVE-2021-3679)

Alexey Kardashevskiy discovered that the KVM implementation for PowerPC systems in the Linux kernel did not properly validate RTAS arguments in some situations. An attacker in a guest vm could use this to cause a denial of service (host OS crash) or possibly execute arbitrary code. (CVE-2021-37576)

It was discovered that the Virtio console implementation in the Linux kernel did not properly validate input lengths in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-38160)

Michael Wakabayashi discovered that the NFSv4 client implementation in the Linux kernel did not properly order connection setup operations. An attacker controlling a remote NFS server could use this to cause a denial of service on the client. (CVE-2021-38199)

It was discovered that the MAX-3421 host USB device driver in the Linux kernel did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-38204)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5091-1>

Solution

Update the affected kernel package.

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

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-2021-3679 |
| CVE | CVE-2021-33624 |
| CVE | CVE-2021-37576 |
| CVE | CVE-2021-38160 |
| CVE | CVE-2021-38199 |
| CVE | CVE-2021-38204 |
| XREF | USN:5091-1 |

Plugin Information

Published: 2021/09/28, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-88-generic for this advisory.

156481 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5210-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5210-1 advisory.

Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. (CVE-2021-4002)

It was discovered that the Linux kernel did not properly enforce certain types of entries in the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. An attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2020-26541)

It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-20321)

It was discovered that the NFC subsystem in the Linux kernel contained a use-after-free vulnerability in its NFC Controller Interface (NCI) implementation. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-3760)

It was discovered that an integer overflow could be triggered in the eBPF implementation in the Linux kernel when preallocating objects for stack maps. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-41864)

It was discovered that the KVM implementation for POWER8 processors in the Linux kernel did not properly keep track if a wakeup event could be resolved by a guest. An attacker in a guest VM could possibly use this to cause a denial of service (host OS crash). (CVE-2021-43056)

It was discovered that the ISDN CAPI implementation in the Linux kernel contained a race condition in certain situations that could trigger an array out-of-bounds bug. A privileged local attacker could possibly use this to cause a denial of service or execute arbitrary code. (CVE-2021-43389)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5210-1>

Solution

Update the affected kernel package.

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

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-2020-26541 |
| CVE | CVE-2021-3760 |
| CVE | CVE-2021-4002 |
| CVE | CVE-2021-20321 |
| CVE | CVE-2021-41864 |
| CVE | CVE-2021-43056 |
| CVE | CVE-2021-43389 |
| XREF | USN:5210-1 |

Plugin Information

Published: 2022/01/06, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-92-generic for this advisory.

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5267-1 advisory.

It was discovered that the Bluetooth subsystem in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3640)

Likang Luo discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3752)

Luo Likang discovered that the FireDTV Firewire driver in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-42739)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5267-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-3640 |
| CVE | CVE-2021-3752 |
| CVE | CVE-2021-42739 |
| XREF | USN:5267-1 |

Plugin Information

Published: 2022/02/03, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-97-generic for this advisory.

159144 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5338-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5338-1 advisory.

Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. (CVE-2022-0492)

Jrgen Gro discovered that the Xen subsystem within the Linux kernel did not adequately limit the number of events driver domains (unprivileged PV backends) could send to other guest VMs. An attacker in a driver domain could use this to cause a denial of service in other guest VMs. (CVE-2021-28711, CVE-2021-28712, CVE-2021-28713)

Jrgen Gro discovered that the Xen network backend driver in the Linux kernel did not adequately limit the amount of queued packets when a guest did not process them. An attacker in a guest VM can use this to cause a denial of service (excessive kernel memory consumption) in the network backend domain. (CVE-2021-28714, CVE-2021-28715)

It was discovered that the simulated networking device driver for the Linux kernel did not properly initialize memory in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-4135)

Brendan Dolan-Gavitt discovered that the Marvell WiFi-Ex USB device driver in the Linux kernel did not properly handle some error conditions. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-43976)

It was discovered that the ARM Trusted Execution Environment (TEE) subsystem in the Linux kernel contained a race condition leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-44733)

It was discovered that the Phone Network protocol (PhoNet) implementation in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45095)

It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45480)

Samuel Page discovered that the Transparent Inter-Process Communication (TIPC) protocol implementation in the Linux kernel contained a stack-based buffer overflow. A remote attacker could use this to cause a denial of service (system crash) for systems that have a TIPC bearer configured. (CVE-2022-0435)

It was discovered that the KVM implementation for s390 systems in the Linux kernel did not properly prevent memory operations on PVM guests that were in non-protected mode. A local attacker could use this to obtain unauthorized memory write access. (CVE-2022-0516)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5338-1>

Solution

Update the affected kernel package.

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

8.2 (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-2021-4135 |
| CVE | CVE-2021-28711 |
| CVE | CVE-2021-28712 |
| CVE | CVE-2021-28713 |
| CVE | CVE-2021-28714 |
| CVE | CVE-2021-28715 |
| CVE | CVE-2021-43976 |
| CVE | CVE-2021-44733 |
| CVE | CVE-2021-45095 |
| CVE | CVE-2021-45480 |
| CVE | CVE-2022-0435 |
| CVE | CVE-2022-0492 |
| CVE | CVE-2022-0516 |
| XREF | USN:5338-1 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/03/22, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-105-generic for this advisory.

161810 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5442-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5442-1 advisory.

Kyle Zeng discovered that the Network Queuing and Scheduling subsystem of the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.
(CVE-2022-29581)

Bing-Jhong Billy Jheng discovered that the io_uring subsystem in the Linux kernel contained an integer overflow. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1116)

Jann Horn discovered that the Linux kernel did not properly enforce seccomp restrictions in some situations. A local attacker could use this to bypass intended seccomp sandbox restrictions.
(CVE-2022-30594)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5442-1>

Solution

Update the affected kernel package.

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

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-2022-1116 |
| CVE | CVE-2022-29581 |
| CVE | CVE-2022-30594 |
| XREF | USN:5442-1 |

Plugin Information

Published: 2022/06/03, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-113-generic for this advisory.

161950 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5467-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5467-1 advisory.

It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2022-21499)

Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1966)

It was discovered that the SCTP protocol implementation in the Linux kernel did not properly verify VTAGs in some situations. A remote attacker could possibly use this to cause a denial of service (connection disassociation). (CVE-2021-3772)

Eric Biederman discovered that the cgroup process migration implementation in the Linux kernel did not perform permission checks correctly in some situations. A local attacker could possibly use this to gain administrative privileges. (CVE-2021-4197)

Jann Horn discovered that the FUSE file system in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1011)

Qiuaho Li, Gaoning Pan and Yongkang Jia discovered that the KVM implementation in the Linux kernel did not properly perform guest page table updates in some situations. An attacker in a guest vm could possibly use this to crash the host OS. (CVE-2022-1158)

Duoming Zhou discovered that the 6pack protocol implementation in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-1198)

It was discovered that the PF_KEYv2 implementation in the Linux kernel did not properly initialize kernel memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-1353)

It was discovered that the implementation of X.25 network protocols in the Linux kernel did not terminate link layer sessions properly. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1516)

Demi Marie Obenour and Simon Gaiser discovered that several Xen para- virtualization device frontends did not properly restrict the access rights of device backends. An attacker could possibly use a malicious Xen backend to gain access to memory pages of a guest VM or cause a denial of service in the guest. (CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042)

It was discovered that the USB Gadget file system interface in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-24958)

It was discovered that the USB SR9700 ethernet device driver for the Linux kernel did not properly validate the length of requests from the device. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-26966)

discovered that the 802.2 LLC type 2 driver in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could use this to cause a denial of service. (CVE-2022-28356)

It was discovered that the Microchip CAN BUS Analyzer interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-28389)

It was discovered that the EMS CAN/USB interface implementation in the Linux kernel contained a double-free vulnerability when handling certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-28390)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5467-1>

Solution

Update the affected kernel package.

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

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-2021-3772 |
| CVE | CVE-2021-4197 |
| CVE | CVE-2022-1011 |
| CVE | CVE-2022-1158 |
| CVE | CVE-2022-1198 |
| CVE | CVE-2022-1353 |
| CVE | CVE-2022-1516 |
| CVE | CVE-2022-21499 |
| CVE | CVE-2022-23036 |
| CVE | CVE-2022-23037 |
| CVE | CVE-2022-23038 |
| CVE | CVE-2022-23039 |
| CVE | CVE-2022-23040 |
| CVE | CVE-2022-23041 |
| CVE | CVE-2022-23042 |
| CVE | CVE-2022-24958 |
| CVE | CVE-2022-26966 |
| CVE | CVE-2022-28356 |
| CVE | CVE-2022-28389 |
| CVE | CVE-2022-28390 |
| XREF | USN:5467-1 |

Plugin Information

Published: 2022/06/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-117-generic for this advisory.
```

164036 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5562-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5562-1 advisory.

Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2588)

It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2586)

It was discovered that the block layer subsystem in the Linux kernel did not properly initialize memory in some situations. A privileged local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-0494)

Hu Jiahui discovered that multiple race conditions existed in the Advanced Linux Sound Architecture (ALSA) framework, leading to use-after-free vulnerabilities. A local attacker could use these to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1048)

Minh Yuan discovered that the floppy disk driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1652)

It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1679)

It was discovered that the Marvell NFC device driver implementation in the Linux kernel did not properly perform memory cleanup operations in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1734)

Duoming Zhou discovered a race condition in the NFC subsystem in the Linux kernel, leading to a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1974)

Duoming Zhou discovered that the NFC subsystem in the Linux kernel did not properly prevent context switches from occurring during certain atomic context operations. A privileged local attacker could use this to cause a denial of service (system crash). (CVE-2022-1975)

Felix Fu discovered that the Sun RPC implementation in the Linux kernel did not properly handle socket states, leading to a use-after-free vulnerability. A remote attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-28893)

Arthur Mongodin discovered that the netfilter subsystem in the Linux kernel did not properly perform data validation. A local attacker could use this to escalate privileges in certain situations. (CVE-2022-34918)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5562-1>

Solution

Update the affected kernel package.

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

7.5 (CVSS:3.0/E:H/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

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2022-0494 |
| CVE | CVE-2022-1048 |
| CVE | CVE-2022-1652 |
| CVE | CVE-2022-1679 |
| CVE | CVE-2022-1734 |
| CVE | CVE-2022-1974 |
| CVE | CVE-2022-1975 |
| CVE | CVE-2022-2586 |
| CVE | CVE-2022-2588 |
| CVE | CVE-2022-28893 |
| CVE | CVE-2022-34918 |
| XREF | USN:5562-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/07/17 |

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2022/08/10, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-124-generic for this advisory.

166286 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5691-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5691-1 advisory.

David Bouman and Billy Jheng Bing Jhong discovered that a race condition existed in the io_uring subsystem in the Linux kernel, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2602)

Snke Huster discovered that an integer overflow vulnerability existed in the WiFi driver stack in the Linux kernel, leading to a buffer overflow. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41674)

Snke Huster discovered that the WiFi driver stack in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42720)

Snke Huster discovered that the WiFi driver stack in the Linux kernel did not properly handle BSSID/SSID lists in some situations. A physically proximate attacker could use this to cause a denial of service (infinite loop). (CVE-2022-42721)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5691-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-2602 |
| CVE | CVE-2022-41674 |
| CVE | CVE-2022-42720 |
| CVE | CVE-2022-42721 |
| XREF | USN:5691-1 |

Plugin Information

Published: 2022/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-131-generic for this advisory.

171261 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5853-1 advisory.

It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3628)

It was discovered that a use-after-free vulnerability existed in the Bluetooth stack in the Linux kernel.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3640)

Khalid Masum discovered that the NILFS2 file system implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-3649)

It was discovered that a race condition existed in the SMSC UFX USB driver implementation in the Linux kernel, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41849)

It was discovered that a race condition existed in the Roccat HID driver in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41850)

Tams Koczka discovered that the Bluetooth L2CAP implementation in the Linux kernel did not properly initialize memory in some situations. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-42895)

It was discovered that the binder IPC implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-20928)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5853-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-3628 |
| CVE | CVE-2022-3640 |
| CVE | CVE-2022-3649 |
| CVE | CVE-2022-41849 |
| CVE | CVE-2022-41850 |
| CVE | CVE-2022-42895 |
| CVE | CVE-2023-20928 |
| XREF | USN:5853-1 |

Plugin Information

Published: 2023/02/09, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-139-generic for this advisory.

172135 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory.

It was discovered that the Upper Level Protocol (ULP) subsystem in the Linux kernel did not properly handle sockets entering the LISTEN state in certain protocols, leading to a use-after-free vulnerability.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0461)

It was discovered that the NVMe driver in the Linux kernel did not properly handle reset events in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3169)

It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3424)

Gwangun Jung discovered a race condition in the IPv4 implementation in the Linux kernel when deleting multipath routes, resulting in an out-of-bounds read. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3435)

It was discovered that a race condition existed in the Kernel Connection Multiplexor (KCM) socket implementation in the Linux kernel when releasing sockets in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3521)

It was discovered that the Netronome Ethernet driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3545)

It was discovered that the hugetlb implementation in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2022-3623)

Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-36280)

Hyunwoo Kim discovered that the DVB Core driver in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41218)

It was discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-4139)

It was discovered that a race condition existed in the Xen network backend driver in the Linux kernel when handling dropped packets in certain circumstances. An attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-42328, CVE-2022-42329)

It was discovered that the Atmel WILC1000 driver in the Linux kernel did not properly validate offsets, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash). (CVE-2022-47520)

It was discovered that the network queuing discipline implementation in the Linux kernel contained a null pointer dereference in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-47929)

Jos Oliveira and Rodrigo Branco discovered that the prctl syscall implementation in the Linux kernel did not properly protect against indirect branch prediction attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-0045)

It was discovered that a use-after-free vulnerability existed in the Advanced Linux Sound Architecture (ALSA) subsystem. A local attacker could use this to cause a denial of service (system crash).

(CVE-2023-0266)

Kyle Zeng discovered that the IPv6 implementation in the Linux kernel contained a NULL pointer dereference vulnerability in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-0394)

It was discovered that the Android Binder IPC subsystem in the Linux kernel did not properly validate inputs in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-20938)

Kyle Zeng discovered that the class-based queuing discipline implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-23454)

Kyle Zeng discovered that the ATM VC queuing discipline implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-23455)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5917-1>

Solution

Update the affected kernel package.

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

7.2 (CVSS:3.0/E:F/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

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2022-3169 |
| CVE | CVE-2022-3424 |
| CVE | CVE-2022-3435 |
| CVE | CVE-2022-3521 |
| CVE | CVE-2022-3545 |
| CVE | CVE-2022-3623 |
| CVE | CVE-2022-4139 |
| CVE | CVE-2022-36280 |
| CVE | CVE-2022-41218 |
| CVE | CVE-2022-42328 |
| CVE | CVE-2022-42329 |
| CVE | CVE-2022-47520 |
| CVE | CVE-2022-47929 |
| CVE | CVE-2023-0045 |
| CVE | CVE-2023-0266 |
| CVE | CVE-2023-0394 |
| CVE | CVE-2023-0461 |
| CVE | CVE-2023-20938 |
| CVE | CVE-2023-23454 |
| CVE | CVE-2023-23455 |
| XREF | USN:5917-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/04/20 |

Plugin Information

Published: 2023/03/06, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-144-generic for this advisory.

190874 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6648-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6648-1 advisory.

It was discovered that a race condition existed in the AppleTalk networking subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51781)

Zhenghan Wang discovered that the generic ID allocator implementation in the Linux kernel did not properly check for null bitmap when releasing IDs. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-6915)

Robert Morris discovered that the CIFS network file system implementation in the Linux kernel did not properly validate certain server commands fields, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2024-0565)

Jann Horn discovered that the TLS subsystem in the Linux kernel did not properly handle spliced messages, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-0646)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6648-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-6915 |
| CVE | CVE-2023-51781 |
| CVE | CVE-2024-0565 |
| CVE | CVE-2024-0646 |
| XREF | USN:6648-1 |

Plugin Information

Published: 2024/02/22, Modified: 2024/08/28

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-172-generic for this advisory.

205223 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6951-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;
- M68K architecture;
- User-Mode Linux (UML);
- x86 architecture;
- Accessibility subsystem;
- Character device driver;
- Clock framework and drivers;
- CPU frequency scaling framework;
- Hardware crypto device drivers;
- Buffer Sharing and Synchronization framework;
- FireWire subsystem;
- GPU drivers;
- HW tracing;
- Macintosh device drivers;
- Multiple devices driver;
- Media drivers;
- Network drivers;
- Pin controllers subsystem;
- S/390 drivers;
- SCSI drivers;
- SoundWire subsystem;
- Greybus lights staging drivers;
- TTY drivers;
- Framebuffer layer;
- Virtio drivers;
- 9P distributed file system;
- eCrypt file system;
- EROFS file system;
- Ext4 file system;
- F2FS file system;
- JFFS2 file system;
- Network file system client;
- NILFS2 file system;
- SMB network file system;

- Kernel debugger infrastructure;
- IRQ subsystem;
- Tracing infrastructure;
- Dynamic debug library;
- 9P file system network protocol;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Netfilter;
- NET/ROM layer;
- NFC subsystem;
- NSH protocol;
- Open vSwitch;
- Phonet protocol;
- TIPC protocol;
- Unix domain sockets;
- Wireless networking;
- eXpress Data Path;
- XFRM subsystem;

- ALSA framework; (CVE-2024-36934, CVE-2024-38578, CVE-2024-38600, CVE-2024-27399, CVE-2024-39276, CVE-2024-38596, CVE-2024-36933, CVE-2024-36919, CVE-2024-35976, CVE-2024-37356, CVE-2023-52585, CVE-2024-38558, CVE-2024-38560, CVE-2024-38634, CVE-2024-36959, CVE-2024-38633, CVE-2024-36886, CVE-2024-27398, CVE-2024-39493, CVE-2024-26886, CVE-2024-31076, CVE-2024-38559, CVE-2024-38615, CVE-2024-36971, CVE-2024-38627, CVE-2024-36964, CVE-2024-38780, CVE-2024-37353, CVE-2024-38621, CVE-2024-36883, CVE-2024-39488, CVE-2024-38661, CVE-2024-36939, CVE-2024-38589, CVE-2024-38565, CVE-2024-38381, CVE-2024-35947, CVE-2024-36905, CVE-2022-48772, CVE-2024-36017, CVE-2024-36946, CVE-2024-27401, CVE-2024-38579, CVE-2024-38612, CVE-2024-38598, CVE-2024-38635, CVE-2024-38587, CVE-2024-38567, CVE-2024-38549, CVE-2024-36960, CVE-2023-52752, CVE-2024-27019, CVE-2024-38601, CVE-2024-39489, CVE-2024-39467, CVE-2023-52882, CVE-2024-38583, CVE-2024-39480, CVE-2024-38607, CVE-2024-36940, CVE-2024-38659, CVE-2023-52434, CVE-2024-36015, CVE-2024-38582, CVE-2024-36950, CVE-2024-38552, CVE-2024-33621, CVE-2024-36954, CVE-2024-39475, CVE-2024-39301, CVE-2024-38599, CVE-2024-36902, CVE-2024-36286, CVE-2024-38613, CVE-2024-38637, CVE-2024-36941, CVE-2024-36014, CVE-2024-38618, CVE-2024-36904, CVE-2024-36270, CVE-2024-39292, CVE-2024-39471, CVE-2022-48674)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6951-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2022-48674
CVE-2022-48772
CVE-2023-52434
CVE-2023-52585
CVE-2023-52752
CVE-2023-52882
CVE-2024-26886
CVE-2024-27019
CVE-2024-27398
CVE-2024-27399
CVE-2024-27401
CVE-2024-31076
CVE-2024-33621
CVE-2024-35947
CVE-2024-35976
CVE-2024-36014
CVE-2024-36015
CVE-2024-36017
CVE-2024-36270
CVE-2024-36286
CVE-2024-36883
CVE-2024-36886
CVE-2024-36902
CVE-2024-36904
CVE-2024-36905
CVE-2024-36919
CVE-2024-36933
CVE-2024-36934
CVE-2024-36939
CVE-2024-36940
CVE-2024-36941
CVE-2024-36946
CVE-2024-36950
CVE-2024-36954
CVE-2024-36959
CVE-2024-36960
CVE-2024-36964
CVE-2024-36971
CVE-2024-37353
CVE-2024-37356
CVE-2024-38381
CVE-2024-38549
CVE-2024-38552
CVE-2024-38558
CVE-2024-38559
CVE-2024-38560
CVE-2024-38565
CVE-2024-38567
CVE-2024-38578
CVE-2024-38579
CVE-2024-38582
CVE-2024-38583
CVE-2024-38587
CVE-2024-38589
CVE-2024-38596
CVE-2024-38598
CVE-2024-38599
CVE-2024-38600
CVE-2024-38601
CVE-2024-38607
CVE-2024-38612
CVE-2024-38613
CVE-2024-38615
CVE-2024-38618
CVE-2024-38621
CVE-2024-38627
CVE-2024-38633
CVE-2024-38634
CVE-2024-38635
CVE-2024-38637
CVE-2024-38659
CVE-2024-38661
CVE-2024-38780
CVE-2024-39276

| | |
|------|---------------------------------|
| CVE | CVE-2024-39292 |
| CVE | CVE-2024-39301 |
| CVE | CVE-2024-39467 |
| CVE | CVE-2024-39471 |
| CVE | CVE-2024-39475 |
| CVE | CVE-2024-39480 |
| CVE | CVE-2024-39488 |
| CVE | CVE-2024-39489 |
| CVE | CVE-2024-39493 |
| XREF | CISA-KNOWN-EXPLOITED:2024/08/28 |
| XREF | USN:6951-1 |

Plugin Information

Published: 2024/08/08, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-192-generic for this advisory.

210006 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7088-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7088-1 advisory.

Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an integer overflow vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-36402)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;
- PowerPC architecture;
- User-Mode Linux (UML);
- x86 architecture;
- Block layer subsystem;
- Cryptographic API;
- Android drivers;
- Serial ATA and Parallel ATA drivers;
- ATM drivers;
- Drivers core;
- CPU frequency scaling framework;
- Device frequency scaling framework;
- GPU drivers;
- HID subsystem;
- Hardware monitoring drivers;
- InfiniBand drivers;
- Input Device core drivers;

- IOMMU subsystem;
- IRQ chip drivers;
- ISDN/mISDN subsystem;
- LED subsystem;
- Multiple devices driver;
- Media drivers;
- EEPROM drivers;
- VMware VMCI Driver;
- MMC subsystem;
- Network drivers;
- Near Field Communication (NFC) drivers;
- NVME drivers;
- Device tree and open firmware driver;
- Parport drivers;
- PCI subsystem;
- Pin controllers subsystem;
- Remote Processor subsystem;
- S/390 drivers;
- SCSI drivers;
- QCOM SoC drivers;
- Direct Digital Synthesis drivers;
- TTY drivers;
- Userspace I/O drivers;
- DesignWare USB3 driver;
- USB subsystem;
- BTRFS file system;
- File systems infrastructure;
- Ext4 file system;
- F2FS file system;
- JFS file system;
- NILFS2 file system;
- BPF subsystem;
- Core kernel;
- DMA mapping infrastructure;
- Tracing infrastructure;
- Radix Tree data structure library;
- Kernel userspace event delivery library;

- Objagg library;
- Memory management;
- Amateur Radio drivers;
- Bluetooth subsystem;
- CAN network layer;
- Networking core;
- Ethtool driver;
- IPv4 networking;
- IPv6 networking;
- IUCV driver;
- KCM (Kernel Connection Multiplexor) sockets driver;
- MAC80211 subsystem;
- Netfilter;
- Network traffic control;
- SCTP protocol;
- Sun RPC protocol;
- TIPC protocol;
- TLS protocol;
- Wireless networking;
- AppArmor security module;
- Simplified Mandatory Access Control Kernel framework;
- SoC audio core drivers;
- USB sound devices; (CVE-2024-43894, CVE-2024-46737, CVE-2024-46828, CVE-2024-42244, CVE-2024-46723, CVE-2024-41073, CVE-2024-46756, CVE-2024-42288, CVE-2024-46840, CVE-2024-46771, CVE-2024-46757, CVE-2024-43860, CVE-2024-46747, CVE-2024-41017, CVE-2024-42246, CVE-2024-44988, CVE-2024-42281, CVE-2024-36484, CVE-2024-43856, CVE-2024-47668, CVE-2024-46759, CVE-2024-46744, CVE-2024-42289, CVE-2024-42131, CVE-2024-46679, CVE-2024-42304, CVE-2024-46818, CVE-2024-43858, CVE-2024-44960, CVE-2024-45028, CVE-2024-26885, CVE-2024-46676, CVE-2024-46780, CVE-2024-42310, CVE-2024-44987, CVE-2024-41090, CVE-2024-44954, CVE-2024-45026, CVE-2024-42285, CVE-2023-52614, CVE-2024-27051, CVE-2024-43880, CVE-2024-43839, CVE-2024-43884, CVE-2024-42311, CVE-2024-43893, CVE-2024-41072, CVE-2024-41091, CVE-2024-46758, CVE-2024-41022, CVE-2024-46745, CVE-2024-42305, CVE-2024-46673, CVE-2024-42284, CVE-2024-46844, CVE-2024-46677, CVE-2024-45025, CVE-2024-43861, CVE-2024-43914, CVE-2024-46783, CVE-2024-41012, CVE-2024-44999, CVE-2024-44946, CVE-2024-42276, CVE-2024-46740, CVE-2024-42295, CVE-2024-44947, CVE-2024-41059, CVE-2024-26669, CVE-2024-38602, CVE-2024-42306, CVE-2023-52918, CVE-2024-42297, CVE-2024-42229, CVE-2024-43853, CVE-2024-45006, CVE-2024-44998, CVE-2024-42283, CVE-2024-44952, CVE-2024-46761, CVE-2024-43841, CVE-2024-44944, CVE-2024-42313, CVE-2024-45008, CVE-2024-46714, CVE-2024-41065, CVE-2024-43883, CVE-2024-43867, CVE-2024-42286, CVE-2024-43879, CVE-2024-43846, CVE-2024-42280, CVE-2024-43854, CVE-2021-47212, CVE-2024-35848, CVE-2024-41020, CVE-2024-41068, CVE-2024-45021, CVE-2024-41098, CVE-2024-44965, CVE-2024-43890, CVE-2024-45003, CVE-2024-44969, CVE-2024-41011, CVE-2024-46738, CVE-2024-41071, CVE-2024-26800, CVE-2024-46721, CVE-2024-42292, CVE-2024-41081, CVE-2024-44948, CVE-2023-52531, CVE-2024-26891, CVE-2024-26641, CVE-2024-42287, CVE-2024-46722, CVE-2024-41042, CVE-2024-46675, CVE-2024-46743, CVE-2024-42259, CVE-2024-41015, CVE-2024-43908, CVE-2024-46719, CVE-2024-43871, CVE-2024-46739, CVE-2024-42301, CVE-2024-47659, CVE-2024-42271, CVE-2024-26668, CVE-2024-43835, CVE-2024-46829, CVE-2024-47667, CVE-2024-44995, CVE-2024-47669, CVE-2024-38611, CVE-2024-40929, CVE-2024-46815, CVE-2024-43830, CVE-2024-42309, CVE-2024-41063, CVE-2024-46782, CVE-2024-46777, CVE-2024-42265, CVE-2024-46781, CVE-2024-26607, CVE-2024-41064, CVE-2024-46685, CVE-2024-43882, CVE-2024-44935, CVE-2024-46800, CVE-2024-46822, CVE-2024-46755, CVE-2024-46817, CVE-2024-43829, CVE-2024-46798, CVE-2024-46689, CVE-2024-42290, CVE-2024-46750, CVE-2024-26640, CVE-2024-47663, CVE-2024-41070)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7088-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE-2021-47212
CVE-2022-36402
CVE-2023-52531
CVE-2023-52614
CVE-2023-52918
CVE-2024-26607
CVE-2024-26640
CVE-2024-26641
CVE-2024-26668
CVE-2024-26669
CVE-2024-26800
CVE-2024-26885
CVE-2024-26891
CVE-2024-27051
CVE-2024-35848
CVE-2024-36484
CVE-2024-38602
CVE-2024-38611
CVE-2024-40929
CVE-2024-41011
CVE-2024-41012
CVE-2024-41015
CVE-2024-41017
CVE-2024-41020
CVE-2024-41022
CVE-2024-41042
CVE-2024-41059
CVE-2024-41063
CVE-2024-41064
CVE-2024-41065
CVE-2024-41068
CVE-2024-41070
CVE-2024-41071
CVE-2024-41072
CVE-2024-41073
CVE-2024-41081
CVE-2024-41090
CVE-2024-41091
CVE-2024-41098
CVE-2024-42131
CVE-2024-42229
CVE-2024-42244
CVE-2024-42246
CVE-2024-42259
CVE-2024-42265
CVE-2024-42271
CVE-2024-42276
CVE-2024-42280
CVE-2024-42281
CVE-2024-42283
CVE-2024-42284
CVE-2024-42285
CVE-2024-42286
CVE-2024-42287
CVE-2024-42288
CVE-2024-42289
CVE-2024-42290
CVE-2024-42292

CVE-CVE-2024-42295
CVE-CVE-2024-42297
CVE-CVE-2024-42301
CVE-CVE-2024-42304
CVE-CVE-2024-42305
CVE-CVE-2024-42306
CVE-CVE-2024-42309
CVE-CVE-2024-42310
CVE-CVE-2024-42311
CVE-CVE-2024-42313
CVE-CVE-2024-43829
CVE-CVE-2024-43830
CVE-CVE-2024-43835
CVE-CVE-2024-43839
CVE-CVE-2024-43841
CVE-CVE-2024-43846
CVE-CVE-2024-43853
CVE-CVE-2024-43854
CVE-CVE-2024-43856
CVE-CVE-2024-43858
CVE-CVE-2024-43860
CVE-CVE-2024-43861
CVE-CVE-2024-43867
CVE-CVE-2024-43871
CVE-CVE-2024-43879
CVE-CVE-2024-43880
CVE-CVE-2024-43882
CVE-CVE-2024-43883
CVE-CVE-2024-43884
CVE-CVE-2024-43890
CVE-CVE-2024-43893
CVE-CVE-2024-43894
CVE-CVE-2024-43908
CVE-CVE-2024-43914
CVE-CVE-2024-44935
CVE-CVE-2024-44944
CVE-CVE-2024-44946
CVE-CVE-2024-44947
CVE-CVE-2024-44948
CVE-CVE-2024-44952
CVE-CVE-2024-44954
CVE-CVE-2024-44960
CVE-CVE-2024-44965
CVE-CVE-2024-44969
CVE-CVE-2024-44987
CVE-CVE-2024-44988
CVE-CVE-2024-44995
CVE-CVE-2024-44998
CVE-CVE-2024-44999
CVE-CVE-2024-45003
CVE-CVE-2024-45006
CVE-CVE-2024-45008
CVE-CVE-2024-45021
CVE-CVE-2024-45025
CVE-CVE-2024-45026
CVE-CVE-2024-45028
CVE-CVE-2024-46673
CVE-CVE-2024-46675
CVE-CVE-2024-46676
CVE-CVE-2024-46677
CVE-CVE-2024-46679
CVE-CVE-2024-46685
CVE-CVE-2024-46689
CVE-CVE-2024-46714
CVE-CVE-2024-46719
CVE-CVE-2024-46721
CVE-CVE-2024-46722
CVE-CVE-2024-46723
CVE-CVE-2024-46737
CVE-CVE-2024-46738
CVE-CVE-2024-46739
CVE-CVE-2024-46740
CVE-CVE-2024-46743
CVE-CVE-2024-46744
CVE-CVE-2024-46745
CVE-CVE-2024-46747
CVE-CVE-2024-46750
CVE-CVE-2024-46755
CVE-CVE-2024-46756
CVE-CVE-2024-46757
CVE-CVE-2024-46758
CVE-CVE-2024-46759

| | |
|------|----------------|
| CVE | CVE-2024-46761 |
| CVE | CVE-2024-46771 |
| CVE | CVE-2024-46777 |
| CVE | CVE-2024-46780 |
| CVE | CVE-2024-46781 |
| CVE | CVE-2024-46782 |
| CVE | CVE-2024-46783 |
| CVE | CVE-2024-46798 |
| CVE | CVE-2024-46800 |
| CVE | CVE-2024-46815 |
| CVE | CVE-2024-46817 |
| CVE | CVE-2024-46818 |
| CVE | CVE-2024-46822 |
| CVE | CVE-2024-46828 |
| CVE | CVE-2024-46829 |
| CVE | CVE-2024-46840 |
| CVE | CVE-2024-46844 |
| CVE | CVE-2024-47659 |
| CVE | CVE-2024-47663 |
| CVE | CVE-2024-47667 |
| CVE | CVE-2024-47668 |
| CVE | CVE-2024-47669 |
| XREF | USN:7088-1 |

Plugin Information

Published: 2024/10/31, Modified: 2024/10/31

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-200-generic for this advisory.

216774 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7293-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7293-1 advisory.

Attila Szsz discovered that the HFS+ file system implementation in the Linux Kernel contained a heap overflow vulnerability. An attacker could use a specially crafted file system image that, when mounted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2025-0927)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;
- Block layer subsystem;
- ACPI drivers;
- Drivers core;
- ATA over ethernet (AOE) driver;
- TPM device driver;
- GPIO subsystem;
- GPU drivers;
- HID subsystem;
- I2C subsystem;
- InfiniBand drivers;
- Mailbox framework;

- Multiple devices driver;
- Media drivers;
- Network drivers;
- NTB driver;
- Virtio pmem driver;
- Parport drivers;
- PCI subsystem;
- SPI subsystem;
- Direct Digital Synthesis drivers;
- USB Device Class drivers;
- USB Dual Role (OTG-ready) Controller drivers;
- USB Serial drivers;
- USB Type-C support driver;
- Framebuffer layer;
- BTRFS file system;
- Ceph distributed file system;
- Ext4 file system;
- F2FS file system;
- File systems infrastructure;
- JFS file system;
- Network file system (NFS) client;
- Network file system (NFS) server daemon;
- NILFS2 file system;
- SMB network file system;
- Network traffic control;
- Network sockets;
- TCP network protocol;
- BPF subsystem;
- Perf events;
- Arbitrary resource management;
- Timer subsystem drivers;
- Tracing infrastructure;
- Closures library;
- Memory management;
- Amateur Radio drivers;
- Bluetooth subsystem;
- Ethernet bridge;

- CAN network layer;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- MAC80211 subsystem;
- Netfilter;
- Netlink;
- SCTP protocol;
- TIPC protocol;
- Wireless networking;
- XFRM subsystem;
- Key management;
- FireWire sound drivers;
- AudioScience HPI driver;
- Amlogic Meson SoC drivers;
- KVM core; (CVE-2024-50184, CVE-2024-47706, CVE-2024-49962, CVE-2024-35887, CVE-2024-53101, CVE-2024-50199, CVE-2024-47709, CVE-2024-50074, CVE-2024-41066, CVE-2024-42252, CVE-2024-43863, CVE-2024-47685, CVE-2024-47756, CVE-2024-50282, CVE-2024-50143, CVE-2024-50116, CVE-2024-47699, CVE-2024-47698, CVE-2024-50301, CVE-2024-47723, CVE-2024-50296, CVE-2024-50007, CVE-2024-49952, CVE-2024-50233, CVE-2023-52458, CVE-2024-53063, CVE-2024-49975, CVE-2024-50099, CVE-2024-47742, CVE-2024-50033, CVE-2024-50218, CVE-2024-50096, CVE-2024-49981, CVE-2024-40911, CVE-2024-47697, CVE-2024-49894, CVE-2024-49955, CVE-2024-53104, CVE-2024-49963, CVE-2024-49883, CVE-2024-47710, CVE-2024-49959, CVE-2024-49948, CVE-2024-50302, CVE-2024-49867, CVE-2024-50234, CVE-2024-49902, CVE-2024-50006, CVE-2024-47672, CVE-2024-50202, CVE-2024-49851, CVE-2024-35896, CVE-2024-50150, CVE-2024-53061, CVE-2024-46854, CVE-2024-50279, CVE-2024-50278, CVE-2024-50180, CVE-2024-50148, CVE-2024-50194, CVE-2024-50008, CVE-2024-47740, CVE-2024-49938, CVE-2024-46853, CVE-2024-50134, CVE-2024-44931, CVE-2024-46849, CVE-2024-49973, CVE-2024-50142, CVE-2024-49879, CVE-2024-50269, CVE-2024-50230, CVE-2024-49896, CVE-2024-49985, CVE-2024-50151, CVE-2024-40965, CVE-2024-50251, CVE-2024-49995, CVE-2024-47713, CVE-2023-52917, CVE-2024-50205, CVE-2024-49900, CVE-2024-49877, CVE-2024-47679, CVE-2024-50040, CVE-2024-47701, CVE-2024-50168, CVE-2024-49882, CVE-2024-50059, CVE-2024-49958, CVE-2024-50171, CVE-2021-47469, CVE-2024-50024, CVE-2024-47749, CVE-2024-50236, CVE-2024-50127, CVE-2024-50290, CVE-2024-47692, CVE-2024-50167, CVE-2024-49944, CVE-2024-50262, CVE-2024-47674, CVE-2024-49957, CVE-2024-50237, CVE-2024-47712, CVE-2024-49949, CVE-2024-40953, CVE-2024-50267, CVE-2024-53059, CVE-2024-49966, CVE-2024-47737, CVE-2024-49868, CVE-2024-50179, CVE-2024-50035, CVE-2024-49997, CVE-2024-50044, CVE-2024-49903, CVE-2024-46731, CVE-2024-49965, CVE-2024-50287, CVE-2024-50265, CVE-2024-47696, CVE-2024-47670, CVE-2024-47684, CVE-2024-41016, CVE-2024-49878, CVE-2024-49924, CVE-2024-50082, CVE-2024-50273, CVE-2024-38544, CVE-2024-47747, CVE-2024-50299, CVE-2024-50195, CVE-2024-50131, CVE-2024-50039, CVE-2024-49982, CVE-2024-49892, CVE-2024-50229, CVE-2024-50117, CVE-2024-49860, CVE-2024-47757, CVE-2024-53066, CVE-2024-47671, CVE-2024-50045)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7293-1>

Solution

Update the affected kernel package.

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

8.4 (CVSS:3.0/E:F/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

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

References

CVE-2021-47469
CVE-2023-52458
CVE-2023-52917
CVE-2024-35887
CVE-2024-35896
CVE-2024-38544
CVE-2024-40911
CVE-2024-40953
CVE-2024-40965
CVE-2024-41016
CVE-2024-41066
CVE-2024-42252
CVE-2024-43863
CVE-2024-44931
CVE-2024-46731
CVE-2024-46849
CVE-2024-46853
CVE-2024-46854
CVE-2024-47670
CVE-2024-47671
CVE-2024-47672
CVE-2024-47674
CVE-2024-47679
CVE-2024-47684
CVE-2024-47685
CVE-2024-47692
CVE-2024-47696
CVE-2024-47697
CVE-2024-47698
CVE-2024-47699
CVE-2024-47701
CVE-2024-47706
CVE-2024-47709
CVE-2024-47710
CVE-2024-47712
CVE-2024-47713
CVE-2024-47723
CVE-2024-47737
CVE-2024-47740
CVE-2024-47742
CVE-2024-47747
CVE-2024-47749
CVE-2024-47756
CVE-2024-47757
CVE-2024-49851
CVE-2024-49860
CVE-2024-49867
CVE-2024-49868
CVE-2024-49877
CVE-2024-49878
CVE-2024-49879
CVE-2024-49882
CVE-2024-49883
CVE-2024-49892
CVE-2024-49894
CVE-2024-49896
CVE-2024-49900
CVE-2024-49902
CVE-2024-49903
CVE-2024-49924
CVE-2024-49938
CVE-2024-49944
CVE-2024-49948
CVE-2024-49949
CVE-2024-49952
CVE-2024-49955
CVE-2024-49957
CVE-2024-49958
CVE-2024-49959
CVE-2024-49962
CVE-2024-49963
CVE-2024-49965
CVE-2024-49966
CVE-2024-49973
CVE-2024-49975

CVE CVE-2024-49981
CVE CVE-2024-49982
CVE CVE-2024-49985
CVE CVE-2024-49995
CVE CVE-2024-49997
CVE CVE-2024-50006
CVE CVE-2024-50007
CVE CVE-2024-50008
CVE CVE-2024-50024
CVE CVE-2024-50033
CVE CVE-2024-50035
CVE CVE-2024-50039
CVE CVE-2024-50040
CVE CVE-2024-50044
CVE CVE-2024-50045
CVE CVE-2024-50059
CVE CVE-2024-50074
CVE CVE-2024-50082
CVE CVE-2024-50096
CVE CVE-2024-50099
CVE CVE-2024-50116
CVE CVE-2024-50117
CVE CVE-2024-50127
CVE CVE-2024-50131
CVE CVE-2024-50134
CVE CVE-2024-50142
CVE CVE-2024-50143
CVE CVE-2024-50148
CVE CVE-2024-50150
CVE CVE-2024-50151
CVE CVE-2024-50167
CVE CVE-2024-50168
CVE CVE-2024-50171
CVE CVE-2024-50179
CVE CVE-2024-50180
CVE CVE-2024-50184
CVE CVE-2024-50194
CVE CVE-2024-50195
CVE CVE-2024-50199
CVE CVE-2024-50202
CVE CVE-2024-50205
CVE CVE-2024-50218
CVE CVE-2024-50229
CVE CVE-2024-50230
CVE CVE-2024-50233
CVE CVE-2024-50234
CVE CVE-2024-50236
CVE CVE-2024-50237
CVE CVE-2024-50251
CVE CVE-2024-50262
CVE CVE-2024-50265
CVE CVE-2024-50267
CVE CVE-2024-50269
CVE CVE-2024-50273
CVE CVE-2024-50278
CVE CVE-2024-50279
CVE CVE-2024-50282
CVE CVE-2024-50287
CVE CVE-2024-50290
CVE CVE-2024-50296
CVE CVE-2024-50299
CVE CVE-2024-50301
CVE CVE-2024-50302
CVE CVE-2024-53059
CVE CVE-2024-53061
CVE CVE-2024-53063
CVE CVE-2024-53066
CVE CVE-2024-53101
CVE CVE-2024-53104
CVE CVE-2025-0927
XREF USN:7293-1
XREF CISA-KNOWN-EXPLOITED:2025/03/25
XREF CISA-KNOWN-EXPLOITED:2025/02/26

Plugin Information

Published: 2025/02/25, Modified: 2025/03/06

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-208-generic for this advisory.

156879 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5240-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5240-1 advisory.

William Liu and Jamie Hill-Daniel discovered that the file system context functionality in the Linux kernel contained an integer underflow vulnerability, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5240-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.8 (CVSS:3.0/E:F/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

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

References

| | |
|------|---|
| CVE | CVE-2022-0185 |
| XREF | USN:5240-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/09/11 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2022/01/20, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-96-generic for this advisory.

152081 - Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-5022-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5022-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.26 in Ubuntu 20.04 LTS and Ubuntu 21.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.35.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-35.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-26.html>
<https://www.oracle.com/security-alerts/cpujul2021.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5022-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (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

II

References

| | |
|-----|---------------|
| CVE | CVE-2021-2339 |
| CVE | CVE-2021-2340 |
| CVE | CVE-2021-2342 |
| CVE | CVE-2021-2352 |
| CVE | CVE-2021-2354 |
| CVE | CVE-2021-2356 |
| CVE | CVE-2021-2357 |
| CVE | CVE-2021-2367 |
| CVE | CVE-2021-2370 |
| CVE | CVE-2021-2372 |
| CVE | CVE-2021-2374 |
| CVE | CVE-2021-2383 |
| CVE | CVE-2021-2384 |
| CVE | CVE-2021-2385 |
| CVE | CVE-2021-2387 |
| CVE | CVE-2021-2389 |
| CVE | CVE-2021-2390 |
| CVE | CVE-2021-2399 |
| CVE | CVE-2021-2402 |
| CVE | CVE-2021-2410 |
| CVE | CVE-2021-2417 |
| CVE | CVE-2021-2418 |
| CVE | CVE-2021-2422 |
| CVE | CVE-2021-2424 |
| CVE | CVE-2021-2425 |
| CVE | CVE-2021-2426 |

| | |
|------|--------------------|
| CVE | CVE-2021-2427 |
| CVE | CVE-2021-2429 |
| CVE | CVE-2021-2437 |
| CVE | CVE-2021-2440 |
| CVE | CVE-2021-2441 |
| XREF | USN:5022-1 |
| XREF | IAVA:2021-A-0333-S |

Plugin Information

Published: 2021/07/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.26-0ubuntu0.20.04.2

155768 - Ubuntu 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-5168-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5168-1 advisory.

Tavis Ormandy discovered that NSS incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5168-1>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools 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-2021-43527 |
| XREF | USN:5168-1 |

Plugin Information

Published: 2021/12/02, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.6

159204 - Ubuntu 18.04 LTS / 20.04 LTS : OpenVPN vulnerability (USN-5347-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5347-1 advisory.

It was discovered that OpenVPN incorrectly handled certain configurations with multiple authentication plugins. A remote attacker could possibly use this issue to bypass authentication using incomplete credentials.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5347-1>

Solution

Update the affected openvpn package.

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-2022-0547 |
| XREF | USN:5347-1 |

Plugin Information

Published: 2022/03/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : openvpn_2.4.7-1ubuntu2
- Fixed package : openvpn_2.4.7-1ubuntu2.20.04.4

156742 - Ubuntu 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-5227-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5227-1 advisory.

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to hang, resulting in a denial of service. (CVE-2021-23437)

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-34552)

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22815)

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. (CVE-2022-22816)

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22817)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5227-1>

Solution

Update the affected 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-2021-23437 |
| CVE | CVE-2021-34552 |
| CVE | CVE-2022-22815 |
| CVE | CVE-2022-22816 |
| CVE | CVE-2022-22817 |
| XREF | USN:5227-1 |

Plugin Information

Published: 2022/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.5

166448 - Ubuntu 18.04 LTS / 20.04 LTS : Pillow vulnerability (USN-5227-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5227-3 advisory.

USN-5227-1 fixed vulnerabilities in Pillow. It was discovered that the fix for CVE-2022-22817 was incomplete. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5227-3>

Solution

Update the affected 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-2022-22817](#)
XREF USN:5227-3

Plugin Information

Published: 2022/10/25, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.6

157112 - Ubuntu 18.04 LTS / 20.04 LTS : PolicyKit vulnerability (USN-5252-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5252-1 advisory.

It was discovered that the PolicyKit pkexec tool incorrectly handled command-line arguments. A local attacker could use this issue to escalate privileges to an administrator.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5252-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-4034 |
| XREF | USN:5252-1 |
| XREF | IAVA:2022-A-0055 |
| XREF | CISA-KNOWN-EXPLOITED:2022/07/18 |

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2022/01/26, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-polkit-1.0_0.105-26ubuntu1
- Fixed package : gir1.2-polkit-1.0_0.105-26ubuntu1.2

- Installed package : libpolkit-agent-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-agent-1-0_0.105-26ubuntu1.2

- Installed package : libpolkit-gobject-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-gobject-1-0_0.105-26ubuntu1.2

- Installed package : policykit-1_0.105-26ubuntu1
- Fixed package : policykit-1_0.105-26ubuntu1.2
```

156961 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5248-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5248-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, conduct header splitting attacks, conduct spoofing attacks, bypass security restrictions, confuse the user, or execute arbitrary code. (CVE-2021-4129, CVE-2021-4140, CVE-2021-29981, CVE-2021-29982, CVE-2021-29987, CVE-2021-29991, CVE-2021-38495, CVE-2021-38496, CVE-2021-38497, CVE-2021-38498, CVE-2021-38500, CVE-2021-38501, CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509, CVE-2021-43534, CVE-2021-43535, CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43656, CVE-2022-22737, CVE-2022-22738, CVE-2022-22739, CVE-2022-22740, CVE-2022-22741, CVE-2022-22742, CVE-2022-22743, CVE-2022-22745, CVE-2022-22747, CVE-2022-22748, CVE-2022-22751)

It was discovered that Thunderbird ignored the configuration to require STARTTLS for an SMTP connection. A person-in-the-middle could potentially exploit this to perform a downgrade attack in order to intercept messages or take control of a session. (CVE-2021-38502)

It was discovered that JavaScript was unexpectedly enabled in the composition area. An attacker could potentially exploit this in combination with another vulnerability, with unspecified impacts.
(CVE-2021-43528)

A buffer overflow was discovered in the Matrix chat library bundled with Thunderbird. An attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2021-44538)

It was discovered that Thunderbird's OpenPGP integration only considered the inner signed message when checking signature validity in a message that contains an additional outer MIME layer. An attacker could potentially exploit this to trick the user into thinking that a message has a valid signature.
(CVE-2021-4126)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5248-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.0 (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)

STIG Severity

I

References

| | |
|-----|--------------------------------|
| CVE | CVE-2021-4126 |
| CVE | CVE-2021-4129 |
| CVE | CVE-2021-4140 |
| CVE | CVE-2021-29981 |
| CVE | CVE-2021-29982 |
| CVE | CVE-2021-29987 |
| CVE | CVE-2021-29991 |
| CVE | CVE-2021-38495 |
| CVE | CVE-2021-38496 |
| CVE | CVE-2021-38497 |
| CVE | CVE-2021-38498 |
| CVE | CVE-2021-38500 |
| CVE | CVE-2021-38501 |
| CVE | CVE-2021-38502 |
| CVE | CVE-2021-38503 |
| CVE | CVE-2021-38504 |
| CVE | CVE-2021-38506 |
| CVE | CVE-2021-38507 |
| CVE | CVE-2021-38508 |
| CVE | CVE-2021-38509 |
| CVE | CVE-2021-43528 |
| CVE | CVE-2021-43534 |
| CVE | CVE-2021-43535 |
| CVE | CVE-2021-43536 |
| CVE | CVE-2021-43537 |
| CVE | CVE-2021-43538 |
| CVE | CVE-2021-43539 |
| CVE | CVE-2021-43541 |
| CVE | CVE-2021-43542 |
| CVE | CVE-2021-43543 |
| CVE | CVE-2021-43545 |

| | |
|------|--------------------|
| CVE | CVE-2021-43546 |
| CVE | CVE-2021-44538 |
| CVE | CVE-2022-22737 |
| CVE | CVE-2022-22738 |
| CVE | CVE-2022-22739 |
| CVE | CVE-2022-22740 |
| CVE | CVE-2022-22741 |
| CVE | CVE-2022-22742 |
| CVE | CVE-2022-22743 |
| CVE | CVE-2022-22745 |
| CVE | CVE-2022-22747 |
| CVE | CVE-2022-22748 |
| CVE | CVE-2022-22751 |
| XREF | USN:5248-1 |
| XREF | IAVA:2021-A-0603-S |
| XREF | IAVA:2021-A-0366-S |
| XREF | IAVA:2021-A-0386-S |
| XREF | IAVA:2021-A-0450-S |
| XREF | IAVA:2021-A-0461-S |
| XREF | IAVA:2021-A-0527-S |
| XREF | IAVA:2021-A-0569-S |
| XREF | IAVA:2022-A-0017-S |
| XREF | IAVA:2021-A-0405-S |

Plugin Information

Published: 2022/01/22, Modified: 2025/03/06

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:91.5.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:91.5.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:91.5.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:91.5.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:91.5.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:91.5.0+build1-0ubuntu0.20.04.1
```

155766 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerability (USN-5168-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5168-2 advisory.

Tavis Ormandy discovered that NSS, included with Thunderbird, incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause Thunderbird to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5168-2>

Solution

Update the affected 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-2021-43527 |
| XREF | USN:5168-2 |

Plugin Information

Published: 2021/12/02, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:78.14.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:78.14.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:78.14.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:78.14.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:78.14.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:78.14.0+build1-0ubuntu0.20.04.2

157143 - Ubuntu 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5247-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5247-1 advisory.

It was discovered that vim incorrectly handled parsing of filenames in its search functionality. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 21.10. (CVE-2021-3973)

It was discovered that vim incorrectly handled memory when opening and searching the contents of certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2021-3974)

It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. (CVE-2021-3984)

It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. (CVE-2021-4019)

It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. (CVE-2021-4069)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5247-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3973 |
| CVE | CVE-2021-3974 |
| CVE | CVE-2021-3984 |
| CVE | CVE-2021-4019 |
| CVE | CVE-2021-4069 |
| XREF | USN:5247-1 |

Plugin Information

Published: 2022/01/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.6
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.6
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.6

139311 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4444-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4444-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4444-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

7.5 (CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS:2.0/E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2020-9862 |
| CVE | CVE-2020-9893 |
| CVE | CVE-2020-9894 |
| CVE | CVE-2020-9895 |
| CVE | CVE-2020-9915 |
| CVE | CVE-2020-9925 |
| XREF | USN:4444-1 |

Plugin Information

Published: 2020/08/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.28.4-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.28.4-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.28.4-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.28.4-0ubuntu0.20.04.1

143269 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4648-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4648-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4648-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.7 (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-2020-9948 |
| CVE | CVE-2020-9951 |
| CVE | CVE-2020-9952 |
| CVE | CVE-2020-9983 |
| CVE | CVE-2020-13753 |
| XREF | USN:4648-1 |

Plugin Information

Published: 2020/11/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.30.3-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.30.3-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.30.3-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.30.3-0ubuntu0.20.04.1

148891 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4894-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4894-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4894-1>

Solution

Update the affected 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

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-2020-27918 |
| CVE | CVE-2020-29623 |
| CVE | CVE-2021-1765 |
| CVE | CVE-2021-1789 |
| CVE | CVE-2021-1799 |
| CVE | CVE-2021-1801 |
| CVE | CVE-2021-1870 |
| XREF | USN:4894-1 |
| XREF | CISA-KNOWN-EXPLOITED:2021/11/17 |
| XREF | CISA-KNOWN-EXPLOITED:2022/05/25 |

Plugin Information

Published: 2021/04/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.30.6-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.30.6-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.30.6-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.30.6-0ubuntu0.20.04.1

149419 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4939-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4939-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4939-1>

Solution

Update the affected 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

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-2021-1788 |
| CVE | CVE-2021-1844 |
| CVE | CVE-2021-1871 |
| XREF | USN:4939-1 |
| XREF | CISA-KNOWN-EXPLOITED:2021/11/17 |

Plugin Information

Published: 2021/05/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.32.0-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.32.0-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.32.0-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.32.0-0ubuntu0.20.04.1

152135 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-5024-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5024-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5024-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-21775 |
| CVE | CVE-2021-21779 |
| CVE | CVE-2021-30663 |
| CVE | CVE-2021-30665 |
| CVE | CVE-2021-30689 |
| CVE | CVE-2021-30720 |
| CVE | CVE-2021-30734 |
| CVE | CVE-2021-30744 |
| CVE | CVE-2021-30749 |
| CVE | CVE-2021-30758 |
| CVE | CVE-2021-30795 |
| CVE | CVE-2021-30797 |
| CVE | CVE-2021-30799 |
| XREF | USN:5024-1 |
| XREF | CISA-KNOWN-EXPLOITED:2021/11/17 |

Plugin Information

Published: 2021/07/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.32.3-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.32.3-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.32.3-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.32.3-0ubuntu0.20.04.1

156076 - Ubuntu 18.04 LTS / 20.04 LTS : X.Org X Server vulnerabilities (USN-5193-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5193-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5193-1>

Solution

Update the affected 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-2021-4008 |
| CVE | CVE-2021-4009 |
| CVE | CVE-2021-4010 |
| CVE | CVE-2021-4011 |
| XREF | USN:5193-1 |

Plugin Information

Published: 2021/12/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.2
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.2
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.2
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.2
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.2

159714 - Ubuntu 18.04 LTS / 20.04 LTS : XZ Utils vulnerability (USN-5378-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5378-2 advisory.

Cleemy Desu Wayo discovered that XZ Utils incorrectly handled certain filenames. If a user or automated system were tricked into performing xzgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5378-2>

Solution

Update the affected 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: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 | USN:5378-2 |
| XREF | IAVA:2024-A-0327 |

Plugin Information

Published: 2022/04/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : liblzma5_5.2.4-1
- Fixed package : liblzma5_5.2.4-1ubuntu1.1
- Installed package : xz-utils_5.2.4-1
- Fixed package : xz-utils_5.2.4-1ubuntu1.1

160028 - Ubuntu 18.04 LTS / 20.04 LTS : libinput vulnerability (USN-5382-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5382-1 advisory.

Albin Eldstl-Ahrens and Lukas Lamster discovered libinput did not properly handle input devices with specially crafted names. A local attacker with physical access could use this to cause libinput to crash or expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5382-1>

Solution

Update the affected 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-2022-1215 |
| XREF | USN:5382-1 |

Plugin Information

Published: 2022/04/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libinput-bin_1.15.5-1
- Fixed package : libinput-bin_1.15.5-1ubuntu0.3
- Installed package : libinput10_1.15.5-1
- Fixed package : libinput10_1.15.5-1ubuntu0.3

150131 - Ubuntu 18.04 LTS / 20.04 LTS : libwebp vulnerabilities (USN-4971-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4971-1 advisory.

It was discovered that libwebp incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4971-1>

Solution

Update the affected 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

8.5 (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-2018-25009 |
| CVE | CVE-2018-25010 |
| CVE | CVE-2018-25011 |
| CVE | CVE-2018-25012 |
| CVE | CVE-2018-25013 |
| CVE | CVE-2018-25014 |
| CVE | CVE-2020-36328 |
| CVE | CVE-2020-36329 |
| CVE | CVE-2020-36330 |
| CVE | CVE-2020-36331 |
| CVE | CVE-2020-36332 |
| XREF | USN:4971-1 |

Plugin Information

Published: 2021/06/01, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libwebp6_0.6.1-2
- Fixed package : libwebp6_0.6.1-2ubuntu0.20.04.1
- Installed package : libwebpdemux2_0.6.1-2
- Fixed package : libwebpdemux2_0.6.1-2ubuntu0.20.04.1
- Installed package : libwebpmux3_0.6.1-2
- Fixed package : libwebpmux3_0.6.1-2ubuntu0.20.04.1

149903 - Ubuntu 18.04 LTS / 20.04 LTS : libx11 vulnerability (USN-4966-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4966-1 advisory.

It was discovered that libx11 incorrectly validated certain parameter lengths. A remote attacker could possibly use this issue to trick libx11 into emitting extra X protocol requests.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4966-1>

Solution

Update the affected 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-2021-31535 |
| XREF | USN:4966-1 |

Plugin Information

Published: 2021/05/25, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libx11-6_2:1.6.9-2ubuntu1
- Fixed package : libx11-6_2:1.6.9-2ubuntu1.2
- Installed package : libx11-data_2:1.6.9-2ubuntu1
- Fixed package : libx11-data_2:1.6.9-2ubuntu1.2
- Installed package : libx11-xcb1_2:1.6.9-2ubuntu1
- Fixed package : libx11-xcb1_2:1.6.9-2ubuntu1.2

186191 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Apache HTTP Server vulnerabilities (USN-6506-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6506-1 advisory.

David Shoon discovered that the Apache HTTP Server mod_macro module incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2023-31122)

Prof. Sven Dietrich, Isa Jafarov, Prof. Heejo Lee, and Choongin Lee discovered that the Apache HTTP Server incorrectly handled certain HTTP/2 connections. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. This issue only affected Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-43622)

Will Dormann and David Warren discovered that the Apache HTTP Server incorrectly handled memory when handling HTTP/2 connections. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. (CVE-2023-45802)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6506-1>

Solution

Update the affected 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-2023-31122 |
| CVE | CVE-2023-43622 |
| CVE | CVE-2023-45802 |
| XREF | USN:6506-1 |
| XREF | IAVA:2023-A-0572-S |

Plugin Information

Published: 2023/11/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.15
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.15

- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.15
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.15

189294 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerabilities (USN-6593-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6593-1 advisory.

It was discovered that GnuTLS had a timing side-channel when processing malformed ciphertexts in RSA-PSK ClientKeyExchange. A remote attacker could possibly use this issue to recover sensitive information.

(CVE-2024-0553)

It was discovered that GnuTLS incorrectly handled certain certificate chains with a cross-signing loop. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service.

This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2024-0567)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6593-1>

Solution

Update the affected 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: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-2024-0553 |
| CVE | CVE-2024-0567 |
| XREF | USN:6593-1 |

Plugin Information

Published: 2024/01/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.10

187626 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : SQLite vulnerabilities (USN-6566-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6566-1 advisory.

It was discovered that SQLite incorrectly handled certain protection mechanisms when using a CLI script with the --safe option, contrary to expectations. This issue only affected Ubuntu 22.04 LTS.

(CVE-2022-46908)

It was discovered that SQLite incorrectly handled certain memory operations in the sessions extension. A remote attacker could possibly use this issue to cause SQLite to crash, resulting in a denial of service.

(CVE-2023-7104)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6566-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.6 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-46908 |
| CVE | CVE-2023-7104 |
| XREF | IAVA:2023-A-0006-S |
| XREF | USN:6566-1 |
| XREF | IAVA:2024-A-0003-S |

Plugin Information

Published: 2024/01/03, Modified: 2025/04/25

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.6

186824 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6555-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6555-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled XKB button actions. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-6377)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the RRChangeOutputProperty and RRChangeProviderProperty APIs. An attacker could possibly use this issue to cause the X Server to crash, or obtain sensitive information. (CVE-2023-6478)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6555-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2023-6377 |
| CVE | CVE-2023-6478 |
| XREF | USN:6555-1 |

Plugin Information

Published: 2023/12/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.12
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.12
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.12
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.12
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.12

186192 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : nghttp2 vulnerability (USN-6505-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6505-1 advisory.

It was discovered that nghttp2 incorrectly handled request cancellation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6505-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-44487 |
| XREF | CISA-KNOWN-EXPLOITED:2023/10/31 |
| XREF | USN:6505-1 |
| XREF | CEA-ID:CEA-2024-0004 |

Plugin Information

Published: 2023/11/22, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libnghttp2-14_1.40.0-1build1
- Fixed package : libnghttp2-14_1.40.0-1ubuntu0.2

177476 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Bind vulnerabilities (USN-6183-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6183-1 advisory.

Shoham Danino, Anat Bremler-Barr, Yehuda Afek, and Yuval Shavit discovered that Bind incorrectly handled the cache size limit. A remote attacker could possibly use this issue to consume memory, leading to a denial of service. (CVE-2023-2828)

It was discovered that Bind incorrectly handled the recursive-clients quota. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-2911)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6183-1>

Solution

Update the affected 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 |
| CVE | CVE-2023-2911 |
| XREF | USN:6183-1 |
| XREF | IAVA:2023-A-0320-S |

Plugin Information

Published: 2023/06/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.15
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.15
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.15

181689 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Bind vulnerabilities (USN-6390-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6390-1 advisory.

It was discovered that Bind incorrectly handled certain control channel messages. A remote attacker with access to the control channel could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2023-3341)

Robert Story discovered that Bind incorrectly handled certain DNS-over-TLS queries. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-4236)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6390-1>

Solution

Update the affected 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 |
| CVE | CVE-2023-4236 |
| XREF | USN:6390-1 |
| XREF | IAVA:2023-A-0500-S |

Plugin Information

Published: 2023/09/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.16
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.16
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.16

178108 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Ghostscript vulnerability (USN-6213-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6213-1 advisory.

It was discovered that Ghostscript incorrectly handled pipe devices. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6213-1>

Solution

Update the affected 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-2023-36664 |
| XREF | USN:6213-1 |
| XREF | IAVB:2023-B-0041-S |

Plugin Information

Published: 2023/07/10, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.8
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.8
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.8
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.8

176715 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : LibRaw vulnerabilities (USN-6137-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6137-1 advisory.

It was discovered that LibRaw incorrectly handled photo files. If a user or automated system were tricked into processing a specially crafted photo file, a remote attacker could cause applications linked against LibRaw to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6137-1>

Solution

Update the affected 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-2021-32142
CVE CVE-2023-1729
XREF USN:6137-1

Plugin Information

Published: 2023/06/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libraw19_0.19.5-1ubuntu1
- Fixed package : libraw19_0.19.5-1ubuntu1.2

176670 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Perl vulnerability (USN-6112-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6112-2 advisory.

USN-6112-1 fixed vulnerabilities in Perl. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6112-2>

Solution

Update the affected 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)

References

| | |
|------|----------------|
| CVE | CVE-2023-31484 |
| XREF | USN:6112-2 |

Plugin Information

Published: 2023/06/05, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libperl5.30_5.30.0-9build1
- Fixed package : libperl5.30_5.30.0-9ubuntu0.4
- Installed package : perl_5.30.0-9build1
- Fixed package : perl_5.30.0-9ubuntu0.4
- Installed package : perl-base_5.30.0-9build1
- Fixed package : perl-base_5.30.0-9ubuntu0.4
- Installed package : perl-modules-5.30_5.30.0-9build1
- Fixed package : perl-modules-5.30_5.30.0-9ubuntu0.4

177902 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : ReportLab vulnerability (USN-6196-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6196-1 advisory.

It was discovered that ReportLab incorrectly handled certain PDF files. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6196-1>

Solution

Update the affected python3-renderpm, python3-reportlab and / or python3-reportlab-accel 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:I/C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-33733 |
| XREF | USN:6196-1 |

Plugin Information

Published: 2023/07/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-renderpm_3.5.34-1ubuntu1
- Fixed package : python3-renderpm_3.5.34-1ubuntu1.1
- Installed package : python3-reportlab_3.5.34-1ubuntu1
- Fixed package : python3-reportlab_3.5.34-1ubuntu1.1
- Installed package : python3-reportlab-accel_3.5.34-1ubuntu1
- Fixed package : python3-reportlab-accel_3.5.34-1ubuntu1.1

177356 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libx11 vulnerability (USN-6168-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6168-1 advisory.

Gregory James Duck discovered that libx11 incorrectly handled certain Request, Event, or Error IDs. If a user were tricked into connecting to a malicious X Server, a remote attacker could possibly use this issue to cause libx11 to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6168-1>

Solution

Update the affected 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 |
| XREF | USN:6168-1 |

Plugin Information

Published: 2023/06/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libx11-6_2:1.6.9-2ubuntu1
- Fixed package : libx11-6_2:1.6.9-2ubuntu1.5

- Installed package : libx11-data_2:1.6.9-2ubuntu1
- Fixed package : libx11-data_2:1.6.9-2ubuntu1.5
- Installed package : libx11-xcb1_2:1.6.9-2ubuntu1
- Fixed package : libx11-xcb1_2:1.6.9-2ubuntu1.5

198070 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GStreamer Base Plugins vulnerability (USN-6798-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6798-1 advisory.

It was discovered that GStreamer Base Plugins incorrectly handled certain EXIF metadata. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6798-1>

Solution

Update the affected 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

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-2024-4453 |
| XREF | USN:6798-1 |

Plugin Information

Published: 2024/05/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-gst-plugins-base-1.0_1.16.2-4
- Fixed package : gir1.2-gst-plugins-base-1.0_1.16.3-0ubuntu1.3
- Installed package : gstreamer1.0-alsa_1.16.2-4
- Fixed package : gstreamer1.0-alsa_1.16.3-0ubuntu1.3
- Installed package : gstreamer1.0-gl_1.16.2-4
- Fixed package : gstreamer1.0-gl_1.16.3-0ubuntu1.3
- Installed package : gstreamer1.0-plugins-base_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base_1.16.3-0ubuntu1.3
- Installed package : gstreamer1.0-plugins-base-apps_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base-apps_1.16.3-0ubuntu1.3
- Installed package : gstreamer1.0-x_1.16.2-4

- Fixed package : gstreamer1.0-x_1.16.3-0ubuntu1.3
- Installed package : libgstreamer-glib1.0-0_1.16.2-4
- Fixed package : libgstreamer-glib1.0-0_1.16.3-0ubuntu1.3
- Installed package : libgstreamer-plugins-base1.0-0_1.16.2-4
- Fixed package : libgstreamer-plugins-base1.0-0_1.16.3-0ubuntu1.3

198045 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibreOffice vulnerability (USN-6789-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6789-1 advisory.

Amel Bouziane-Leblond discovered that LibreOffice incorrectly handled graphic on-click bindings. If a user were tricked into clicking a graphic in a specially crafted document, a remote attacker could possibly run arbitrary script.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6789-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-3044 |
| XREF | USN:6789-1 |
| XREF | IAVB:2024-B-0058-S |

Plugin Information

Published: 2024/05/28, Modified: 2024/11/13

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.10
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.10

- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libuno-purenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.10
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.10
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.10
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.10
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.10

200488 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : VTE vulnerability (USN-6833-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6833-1 advisory.

Siddharth Dushantha discovered that VTE incorrectly handled large window resize escape sequences. An attacker could possibly use this issue to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6833-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.9 (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-2024-37535
XREF-USN:6833-1

Plugin Information

Published: 2024/06/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-vte-2.91_0.60.3-0ubuntu1~20.04
- Fixed package : gir1.2-vte-2.91_0.60.3-0ubuntu1~20.5
- Installed package : libvte-2.91-0_0.60.3-0ubuntu1~20.04
- Fixed package : libvte-2.91-0_0.60.3-0ubuntu1~20.5
- Installed package : libvte-2.91-common_0.60.3-0ubuntu1~20.04
- Fixed package : libvte-2.91-common_0.60.3-0ubuntu1~20.5

201043 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Wget vulnerability (USN-6852-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6852-1 advisory.

It was discovered that Wget incorrectly handled semicolons in the userinfo subcomponent of a URI. A remote attacker could possibly trick a user into connecting to a different host than expected.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6852-1>

Solution

Update the affected wget package.

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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2024-38428](#)
XREF USN:6852-1

Plugin Information

Published: 2024/06/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : wget_1.20.3-1ubuntu1
- Fixed package : wget_1.20.3-1ubuntu2.1

200438 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libndp vulnerability (USN-6830-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6830-1 advisory.

It was discovered that libndp incorrectly handled certain malformed IPv6 router advertisement packets. A local attacker could use this issue to cause NetworkManager to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6830-1>

Solution

Update the affected libndp-dev, libndp-tools and / or libndp0 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)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2024-5564 |
| XREF | IAVA:2024-A-0326 |
| XREF | USN:6830-1 |

Plugin Information

Published: 2024/06/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libndp0_1.7-0ubuntu1
- Fixed package : libndp0_1.7-0ubuntu1.1

200175 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libvpx vulnerability (USN-6814-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6814-1 advisory.

Xiantong Hou discovered that libvpx did not properly handle certain malformed media files. If an application using libvpx opened a specially crafted file, a remote attacker could cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6814-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

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:N/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2024-5197](#)
XREF USN:6814-1

Plugin Information

Published: 2024/06/06, Modified: 2025/07/23

Plugin Output

tcp/0

- Installed package : libvpx6_1.8.2-1build1
- Fixed package : libvpx6_1.8.2-1ubuntu0.3

193232 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache HTTP Server vulnerabilities (USN-6729-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6729-1 advisory.

Orange Tsai discovered that the Apache HTTP Server incorrectly handled validating certain input. A remote attacker could possibly use this issue to perform HTTP request splitting attacks. (CVE-2023-38709)

Keran Mu and Jianjun Chen discovered that the Apache HTTP Server incorrectly handled validating certain input. A remote attacker could possibly use this issue to perform HTTP request splitting attacks.
(CVE-2024-24795)

Bartek Nowotarski discovered that the Apache HTTP Server HTTP/2 module incorrectly handled endless continuation frames. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. (CVE-2024-27316)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6729-1>

Solution

Update the affected 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-2023-38709 |
| CVE | CVE-2024-24795 |
| CVE | CVE-2024-27316 |
| XREF | USN:6729-1 |
| XREF | IAVA:2024-A-0202-S |

Plugin Information

Published: 2024/04/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.17
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.17
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.17
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.17

191021 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Dnsmasq vulnerabilities (USN-6657-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6657-1 advisory.

Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner discovered that Dnsmasq incorrectly handled validating DNSSEC messages. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. (CVE-2023-50387)

It was discovered that Dnsmasq incorrectly handled preparing an NSEC3 closest encloser proof. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. (CVE-2023-50868)

It was discovered that Dnsmasq incorrectly set the maximum EDNS.0 UDP packet size as required by DNS Flag Day 2020. This issue only affected Ubuntu 23.10. (CVE-2023-28450)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6657-1>

Solution

Update the affected 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-2023-28450 |
| CVE | CVE-2023-50387 |
| CVE | CVE-2023-50868 |
| XREF | USN:6657-1 |

Plugin Information

Published: 2024/02/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : dnsMasq-base_2.80-1.1ubuntu1
- Fixed package : dnsMasq-base_2.90-0ubuntu0.20.04.1

193515 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6737-1 advisory.

Charles Fol discovered that the GNU C Library iconv feature incorrectly handled certain input sequences.

An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6737-1>

Solution

Update the affected 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 |
|-----|---------------|

XREF

USN:6737-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/04/18, Modified: 2024/10/21

Plugin Output

tcp/0

```
- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.15

- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.15

- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.15

- Installed package : libc6-dev_2.31-0ubuntu9
- Fixed package : libc6-dev_2.31-0ubuntu9.15

- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.15
```

189830 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerabilities (USN-6618-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6618-1 advisory.

It was discovered that Pillow incorrectly handled certain long text arguments. An attacker could possibly use this issue to cause Pillow to consume resources, leading to a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2023-44271)

Duarte Santos discovered that Pillow incorrectly handled the environment parameter to PIL.ImageMath.eval.
An attacker could possibly use this issue to execute arbitrary code. (CVE-2023-50447)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6618-1>

Solution

Update the affected python3-pil and / or python3-pil.imagetk 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-2023-44271](#)

CVE CVE-2023-50447
XREF USN:6618-1

Plugin Information

Published: 2024/01/30, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.8

192119 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : TeX Live vulnerabilities (USN-6695-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6695-1 advisory.

It was discovered that TeX Live incorrectly handled certain memory operations in the embedded axodraw2 tool. An attacker could possibly use this issue to cause TeX Live to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2019-18604)

It was discovered that TeX Live allowed documents to make arbitrary network requests. If a user or automated system were tricked into opening a specially crafted document, a remote attacker could possibly use this issue to exfiltrate sensitive information, or perform other network-related attacks. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2023-32668)

It was discovered that TeX Live incorrectly handled certain TrueType fonts. If a user or automated system were tricked into opening a specially crafted TrueType font, a remote attacker could use this issue to cause TeX Live to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-25262)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6695-1>

Solution

Update the affected 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-2019-18604 |
| CVE | CVE-2023-32668 |
| CVE | CVE-2024-25262 |
| XREF | USN:6695-1 |

Plugin Information

Published: 2024/03/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libkpathsea6_2019.20190605.51237-3build2
- Fixed package : libkpathsea6_2019.20190605.51237-3ubuntu0.2
- Installed package : libsyncTeX2_2019.20190605.51237-3build2
- Fixed package : libsyncTeX2_2019.20190605.51237-3ubuntu0.2

192576 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6717-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6717-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-0743, CVE-2024-2611,

CVE-2024-2614)

Hubert Kario discovered that Thunderbird had a timing side-channel when

performing RSA decryption. A remote attacker could possibly use this

issue to recover sensitive information. (CVE-2023-5388)

Gary Kwong discovered that Thunderbird incorrectly updated return

registers for JIT code on Armv7-A systems. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2024-2607)

Ronald Crane discovered that Thunderbird did not properly manage memory during character encoding. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2608)

Georg Felber and Marco Squarcina discovered that Thunderbird incorrectly

handled html and body tags. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able

obtain sensitive information. (CVE-2024-2610)

Ronald Crane discovered a use-after-free in Thunderbird when handling code in SafeRefPtr. An attacker could potentially exploit this issue to cause a

denial of service, or execute arbitrary code. (CVE-2024-2612)

Ryan VanderMeulen and Dan Minor discovered that Thunderbird did not properly manage memory conditions in ICU. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2616)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6717-1>

Solution

Update the affected 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-2023-5388 |
| CVE | CVE-2024-0743 |
| CVE | CVE-2024-2607 |
| CVE | CVE-2024-2608 |
| CVE | CVE-2024-2610 |
| CVE | CVE-2024-2611 |
| CVE | CVE-2024-2612 |
| CVE | CVE-2024-2614 |
| CVE | CVE-2024-2616 |
| XREF | IAVA:2024-A-0053-S |
| XREF | USN:6717-1 |
| XREF | IAVA:2024-A-0174-S |

Plugin Information

Published: 2024/03/26, Modified: 2025/04/02

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.9.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.9.0+build1-0ubuntu0.20.04.1

193869 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6750-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6750-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-2609, CVE-2024-3852, CVE-2024-3864)

Bartek Nowotarski discovered that Thunderbird did not properly limit HTTP/2 CONTINUATION frames. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3302)

Lukas Bernhard discovered that Thunderbird did not properly manage memory during JIT optimisations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3854)

Lukas Bernhard discovered that Thunderbird did not properly manage memory when handling JIT created code during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3857)

Ronald Crane discovered that Thunderbird did not properly manage memory in the OpenType sanitizer on 32-bit devices, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3859)

Ronald Crane discovered that Thunderbird did not properly manage memory when handling an AlignedBuffer. An attacker could potentially exploit this issue to cause denial of service, or execute arbitrary code.
(CVE-2024-3861)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6750-1>

Solution

Update the affected packages.

Risk Factor

High

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

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-2024-2609 |
| CVE | CVE-2024-3302 |
| CVE | CVE-2024-3852 |
| CVE | CVE-2024-3854 |
| CVE | CVE-2024-3857 |
| CVE | CVE-2024-3859 |
| CVE | CVE-2024-3861 |
| CVE | CVE-2024-3864 |
| XREF | IAVA:2024-A-0174-S |
| XREF | USN:6750-1 |
| XREF | IAVA:2024-A-0257-S |

Plugin Information

Published: 2024/04/25, Modified: 2025/04/02

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.10.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.10.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.10.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.10.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.10.1+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.10.1+build1-0ubuntu0.20.04.1

192621 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6718-1 advisory.

Dan Fandrich discovered that curl would incorrectly use the default set of protocols when a parameter option disabled all protocols without adding any, contrary to expectations. This issue only affected Ubuntu 23.10. (CVE-2024-2004)

It was discovered that curl incorrectly handled memory when limiting the amount of headers when HTTP/2 server push is allowed. A remote attacker could possibly use this issue to cause curl to consume resources, leading to a denial of service. (CVE-2024-2398)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6718-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-2004 |
| CVE | CVE-2024-2398 |
| XREF | USN:6718-1 |
| KREF | IAVA:2024-A-0185-S |

Plugin Information

Published: 2024/03/27, Modified: 2025/07/31

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.22
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.22

191103 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libuv vulnerability (USN-6666-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6666-1 advisory.

It was discovered that libuv incorrectly truncated certain hostnames. A remote attacker could possibly use this issue with specially crafted hostnames to bypass certain checks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6666-1>

Solution

Update the affected libuv1 and / or libuv1-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.6 (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-2024-24806 |
| XREF | USN:6666-1 |

Plugin Information

Published: 2024/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libuv1_1.34.2-1ubuntu1
- Fixed package : libuv1_1.34.2-1ubuntu1.5

237145 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : SQLite vulnerabilities (USN-7528-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7528-1 advisory.

It was discovered that SQLite incorrectly handled the concat_ws() function. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2025-29087, CVE-2025-3277)

It was discovered that SQLite incorrectly handled certain argument values to sqlite3_db_config(). An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-29088)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7528-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

6.9 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/Vl:L/Va:L/SC:L/SI:L/SA:L)

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-2025-3277 |
| CVE | CVE-2025-29087 |
| CVE | CVE-2025-29088 |
| XREF | IAVA:2025-A-0288 |
| XREF | USN:7528-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.7

234777 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Yelp vulnerability (USN-7447-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7447-1 advisory.

It was discovered that Yelp incorrectly handled paths in ghelp URLs. A remote attacker could use this issue to trick users into opening malicious downloaded help files and exfiltrate sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7447-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/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

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2025-3155 |
| XREF | USN:7447-1 |

Plugin Information

Published: 2025/04/23, Modified: 2025/04/24

Plugin Output

tcp/0

- Installed package : libyelp0_3.36.0-1
- Fixed package : libyelp0_3.36.2-0ubuntu1.1
- Installed package : yelp_3.36.0-1
- Fixed package : yelp_3.36.2-0ubuntu1.1
- Installed package : yelp-xsl_3.36.0-1
- Fixed package : yelp-xsl_3.36.0-1ubuntu0.1

214790 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Bind vulnerabilities (USN-7241-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7241-1 advisory.

Toshifumi Sakaguchi discovered that Bind incorrectly handled many records in the additional section. A remote attacker could possibly use this issue to cause Bind to consume CPU resources, leading to a denial of service. (CVE-2024-11187)

Jean-Franois Billaud discovered that the Bind DNS-over-HTTPS implementation incorrectly handled a heavy query load. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. (CVE-2024-12705)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7241-1>

Solution

Update the affected 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-2024-11187 |
| CVE | CVE-2024-12705 |
| XREF | USN:7241-1 |
| XREF | IAVA:2025-A-0071-S |

Plugin Information

Published: 2025/01/29, Modified: 2025/05/22

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.18.30-0ubuntu0.20.04.2
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.18.30-0ubuntu0.20.04.2
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.18.30-0ubuntu0.20.04.2

210776 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Ghostscript vulnerabilities (USN-7103-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7103-1 advisory.

It was discovered that Ghostscript incorrectly handled parsing certain PS files. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-46951, CVE-2024-46953, CVE-2024-46955, CVE-2024-46956)

It was discovered that Ghostscript incorrectly handled parsing certain PDF files. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2024-46952)

It was discovered that Ghostscript incorrectly handled parsing certain PS files. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly bypass file path validation. This issue only affected Ubuntu 24.04 LTS and Ubuntu 24.10. (CVE-2024-46954)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7103-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-46951 |
| CVE | CVE-2024-46952 |
| CVE | CVE-2024-46953 |
| CVE | CVE-2024-46954 |
| CVE | CVE-2024-46955 |
| CVE | CVE-2024-46956 |
| XREF | USN:7103-1 |
| XREF | IAVB:2024-B-0170-S |

Plugin Information

Published: 2024/11/12, Modified: 2025/03/28

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.14
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.14
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.14
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.14

216422 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenSSH vulnerabilities (USN-7270-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7270-1 advisory.

It was discovered that the OpenSSH client incorrectly handled the non-default VerifyHostKeyDNS option. If that option were enabled, an attacker could possibly impersonate a server by completely bypassing the server identity check. (CVE-2025-26465)

It was discovered that OpenSSH incorrectly handled the transport-level ping facility. A remote attacker could possibly use this issue to cause OpenSSH clients and servers to consume resources, leading to a denial of service. This issue only affected Ubuntu 24.04 LTS and Ubuntu 24.10. (CVE-2025-26466)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7270-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.1 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-26465 |
| CVE | CVE-2025-26466 |
| XREF | USN:7270-1 |
| XREF | IAVA:2025-A-0126-S |

Plugin Information

Published: 2025/02/18, Modified: 2025/04/17

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.12
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.12
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.12
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.12

203144 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Bind vulnerabilities (USN-6909-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6909-1 advisory.

It was discovered that Bind incorrectly handled a flood of DNS messages over TCP. A remote attacker could possibly use this issue to cause Bind to become unstable, resulting in a denial of service.
(CVE-2024-0760)

Toshifumi Sakaguchi discovered that Bind incorrectly handled having a very large number of RRs existing at the same time. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. (CVE-2024-1737)

It was discovered that Bind incorrectly handled a large number of SIG(0) signed requests. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service.
(CVE-2024-1975)

Daniel Strnger discovered that Bind incorrectly handled serving both stable cache data and authoritative zone content. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2024-4076)

On Ubuntu 20.04 LTS, Bind has been updated from 9.16 to 9.18. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://kb.isc.org/docs/changes-to-be-aware-of-when-moving-from-bind-916-to-918>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6909-1>

Solution

Update the affected 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-2024-0760 |
| CVE | CVE-2024-1737 |
| CVE | CVE-2024-1975 |
| CVE | CVE-2024-4076 |
| XREF | USN:6909-1 |
| XREF | IAVA:2024-A-0442-S |

Plugin Information

Published: 2024/07/23, Modified: 2025/01/30

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.18.28-0ubuntu0.20.04.1
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.18.28-0ubuntu0.20.04.1
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.18.28-0ubuntu0.20.04.1

207842 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : CUPS vulnerability (USN-7041-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7041-1 advisory.

Simone Margaritelli discovered that CUPS incorrectly sanitized IPP data when creating PPD files. A remote attacker could possibly use this issue to manipulate PPD files and execute arbitrary code when a printer is used.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7041-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.0 (CVSS:3.0/E:F/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

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

References

CVE
XREF

CVE-2024-47175

USN:7041-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/09/27, Modified: 2024/11/25

Plugin Output

tcp/0

```
- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.9

- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.9

- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.9

- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.9

- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.9

- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.9

- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.9

- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.9

- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.9

- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.9

- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.9
```

207953 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Flatpak and Bubblewrap vulnerability (USN-7046-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7046-1 advisory.

It was discovered that Flatpak incorrectly handled certain persisted directories. An attacker could possibly use this issue to read and write files in locations it would not normally have access to. A patch was also needed to Bubblewrap in order to avoid race conditions caused by this fix.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7046-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.7 (CVSS:3.0/E:U/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

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

References

CVE-2024-42472
XREF-USN:7046-1

Plugin Information

Published: 2024/09/30, Modified: 2024/09/30

Plugin Output

tcp/0

- Installed package : bubblewrap_0.4.0-1ubuntu4
- Fixed package : bubblewrap_0.4.0-1ubuntu4.1

205630 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : LibreOffice vulnerability (USN-6962-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6962-1 advisory.

It was discovered that LibreOffice incorrectly allowed users to enable macros when a cryptographic signature failed to validate. If a user were tricked into opening a specially crafted document, a remote attacker could possibly execute arbitrary macros.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6962-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-6472 |
| XREF | USN:6962-1 |
| XREF | IAVB:2024-B-0108-S |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.11
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.11
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.11

```
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libuno-purpenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.11

- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.11

- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.11

- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.11

- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.11
```

204989 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6944-1 advisory.

Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6944-1>

Solution

Update the affected 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-2024-7264 |
| XREF | USN:6944-1 |
| XREF | IAVA:2024-A-0457-S |

Plugin Information

Published: 2024/08/05, Modified: 2024/09/13

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.23
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.23

208701 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : libgsf vulnerabilities (USN-7062-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7062-1 advisory.

It was discovered that libgsf incorrectly handled certain Compound Document Binary files. If a user or automated system were tricked into opening a specially crafted file, a remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7062-1>

Solution

Update the affected 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-2024-36474 |
| CVE | CVE-2024-42415 |
| XREF | USN:7062-1 |

Plugin Information

Published: 2024/10/10, Modified: 2024/10/10

Plugin Output

tcp/0

- Installed package : libgsf-1-114_1.14.46-1
- Fixed package : libgsf-1-114_1.14.46-1ubuntu0.1

- Installed package : libgsf-1-common_1.14.46-1
- Fixed package : libgsf-1-common_1.14.46-1ubuntu0.1

207768 - Ubuntu 20.04 LTS / 22.04 LTS : AppArmor vulnerability (USN-7035-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7035-1 advisory.

It was discovered that the AppArmor policy compiler incorrectly generated looser restrictions than expected for rules allowing mount operations. A local attacker could possibly use this to bypass AppArmor restrictions in applications where some mount operations were permitted.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7035-1>

Solution

Update the affected 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

8.5 (CVSS:3.0/E:U/R:L/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
XREF [CVE-2016-1585](#)
 USN:7035-1

Plugin Information

Published: 2024/09/25, Modified: 2024/09/25

Plugin Output

tcp/0

- Installed package : apparmor_2.13.3-7ubuntu5.1
- Fixed package : apparmor_2.13.3-7ubuntu5.4
- Installed package : libapparmor1_2.13.3-7ubuntu5.1
- Fixed package : libapparmor1_2.13.3-7ubuntu5.4

[170632 - Ubuntu 20.04 LTS / 22.04 LTS : Bind vulnerabilities \(USN-5827-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5827-1 advisory.

Rob Schulhof discovered that Bind incorrectly handled a large number of UPDATE messages. A remote attacker could possibly use this issue to cause Bind to consume resources, resulting in a denial of service.

(CVE-2022-3094)

Borja Marcos discovered that Bind incorrectly handled certain RRSIG queries. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3736)

Maksym Odinintsev discovered that Bind incorrectly handled certain answers from stale cache. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3924)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5827-1>

Solution

Update the affected 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-2022-3094](#)

| | |
|------|--------------------|
| CVE | CVE-2022-3736 |
| CVE | CVE-2022-3924 |
| XREF | USN:5827-1 |
| XREF | IAVA:2023-A-0058-S |

Plugin Information

Published: 2023/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.12
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.12
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.12

214506 - Ubuntu 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-7222-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7222-1 advisory.

Lucas Leong discovered that BlueZ incorrectly handled the Phone Book Access profile. If a user were tricked into connecting to a malicious Bluetooth device, a remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7222-1>

Solution

Update the affected 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-2023-50229 |
| CVE | CVE-2023-50230 |
| XREF | USN:7222-1 |

Plugin Information

Published: 2025/01/22, Modified: 2025/07/09

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.9
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.9
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.9
- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.9

232846 - Ubuntu 20.04 LTS / 22.04 LTS : FreeType vulnerability (USN-7352-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7352-1 advisory.

It was discovered that FreeType incorrectly handled certain memory operations when parsing font subglyph structures. A remote attacker could use this issue to cause FreeType to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7352-1>

Solution

Update the affected 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

7.5 (CVSS:3.0/E:F/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

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

References

| | |
|------|---|
| CVE | CVE-2025-27363 |
| XREF | USN:7352-1 |
| XREF | CISA-KNOWN-EXPLOITED:2025/05/27 |

Plugin Information

Published: 2025/03/19, Modified: 2025/05/06

Plugin Output

tcp/0

- Installed package : libfreetype6_2.10.1-2
- Fixed package : libfreetype6_2.10.1-2ubuntu0.4

177323 - Ubuntu 20.04 LTS / 22.04 LTS : GLib vulnerabilities (USN-6165-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6165-1 advisory.

It was discovered that GLib incorrectly handled non-normal GVariants. An attacker could use this issue to cause GLib to crash, resulting in a denial of service, or perform other unknown attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6165-1>

Solution

Update the affected 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

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-2023-24593 |
| CVE | CVE-2023-25180 |
| CVE | CVE-2023-29499 |
| CVE | CVE-2023-32611 |
| CVE | CVE-2023-32636 |
| CVE | CVE-2023-32643 |
| CVE | CVE-2023-32665 |
| XREF | USN:6165-1 |

Plugin Information

Published: 2023/06/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.6
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.6
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.6

188049 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6581-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6581-1 advisory.

It was discovered that GNU binutils was not properly performing bounds checks in several functions, which could lead to a buffer overflow. An attacker could possibly use this issue to cause a denial of service, expose sensitive information or execute arbitrary code. (CVE-2022-44840, CVE-2022-45703)

It was discovered that GNU binutils incorrectly handled memory management operations in several of its functions, which could lead to excessive memory consumption due to memory leaks. An attacker could possibly use these issues to cause a denial of service.

(CVE-2022-47007, CVE-2022-47008, CVE-2022-47010, CVE-2022-47011)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6581-1>

Solution

Update the affected 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-2022-44840 |
| CVE | CVE-2022-45703 |
| CVE | CVE-2022-47007 |
| CVE | CVE-2022-47008 |
| CVE | CVE-2022-47010 |
| CVE | CVE-2022-47011 |
| XREF | USN:6581-1 |

Plugin Information

Published: 2024/01/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.8
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.8
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.8
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.8
- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.8
- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.8

191003 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6655-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6655-1 advisory.

It was discovered that GNU binutils was not properly handling the logic behind certain memory management related operations, which could lead to an invalid memory access. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-47695)

It was discovered that GNU binutils was not properly performing bounds checks when dealing with memory allocation operations, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-48063)

It was discovered that GNU binutils incorrectly handled memory management operations in several of its functions, which could lead to excessive memory consumption due to memory leaks. An attacker could possibly use these issues to cause a denial of service. (CVE-2022-48065)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6655-1>

Solution

Update the affected 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-2022-47695 |
| CVE | CVE-2022-48063 |
| CVE | CVE-2022-48065 |
| XREF | USN:6655-1 |

Plugin Information

Published: 2024/02/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.9
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.9
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.9
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.9
- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.9

- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.9

171967 - Ubuntu 20.04 LTS / 22.04 LTS : GnuTLS vulnerability (USN-5901-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5901-1 advisory.

Hubert Kario discovered that GnuTLS had a timing side-channel when handling certain RSA messages. A remote attacker could possibly use this issue to recover sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5901-1>

Solution

Update the affected 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 |
| XREF | USN:5901-1 |

Plugin Information

Published: 2023/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.8

214894 - Ubuntu 20.04 LTS / 22.04 LTS : HarfBuzz vulnerability (USN-7251-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7251-1 advisory.

It was discovered that HarfBuzz incorrectly handled shaping certain fonts. A remote attacker could possibly use this issue to cause HarfBuzz to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7251-1>

Solution

Update the affected 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-2023-25193 |
| XREF | USN:7251-1 |

Plugin Information

Published: 2025/02/03, Modified: 2025/02/03

Plugin Output

tcp/0

- Installed package : libharfbuzz-icu0_2.6.4-1ubuntu4
- Fixed package : libharfbuzz-icu0_2.6.4-1ubuntu4.3
- Installed package : libharfbuzz0b_2.6.4-1ubuntu4
- Fixed package : libharfbuzz0b_2.6.4-1ubuntu4.3

176885 - Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerabilities (USN-6144-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6144-1 advisory.

It was discovered that LibreOffice did not properly validate the number of parameters passed to the formula interpreter, leading to an array index underflow attack. If a user were tricked into opening a specially crafted spreadsheet file, an attacker could possibly use this issue to execute arbitrary code. (CVE-2023-0950)

Amel Bouziane-Leblond discovered that LibreOffice did not prompt the user before loading the host document inside an IFrame. If a user were tricked into opening a specially crafted input file, an attacker could possibly use this issue to cause information disclosure or execute arbitrary code. (CVE-2023-2255)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6144-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-0950 |
| CVE | CVE-2023-2255 |
| XREF | USN:6144-1 |
| XREF | IAVB:2023-B-0037-S |

Plugin Information

Published: 2023/06/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.8
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-l10n_de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n_de_1:6.4.7-0ubuntu0.20.04.8

- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libuno-purenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.8
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.8
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.8
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.8
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.8

186989 - Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerabilities (USN-6546-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6546-2 advisory.

USN-6546-1 fixed vulnerabilities in LibreOffice. This update provides the corresponding updates for Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6546-2>

Solution

Update the affected 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:I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2023-6185 |
| CVE | CVE-2023-6186 |
| XREF | USN:6546-2 |

Plugin Information

Published: 2023/12/15, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.9
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.9
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.9

```

- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libuno-purpenhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.9

- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.9

- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.9

- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.9

- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.9

```

207457 - Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerability (USN-7025-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7025-1 advisory.

It was discovered that LibreOffice would incorrectly handle digital signature verification after repairing a corrupted document. A remote attacker could possibly use this issue to forge valid signatures.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7025-1>

Solution

Update the affected 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

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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-7788 |
| XREF | USN:7025-1 |
| XREF | IAVB:2024-B-0136-S |

Plugin Information

Published: 2024/09/19, Modified: 2025/01/17

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.12
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-l10n-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_gb_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.12

- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libuno-purvenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purvenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.12
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.12
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.12
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.12
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.12

183722 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6172-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6172-1 advisory.

It was discovered that the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1076)

It was discovered that the Real-Time Scheduling Class implementation in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1077)

It was discovered that the ASUS HID driver in the Linux kernel did not properly handle device removal, leading to a use-after-free vulnerability. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (system crash). (CVE-2023-1079)

It was discovered that the Xircom PCMCIA network device driver in the Linux kernel did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2023-1670)

It was discovered that a race condition existed in the Xen transport layer implementation for the 9P file system protocol in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (guest crash) or expose sensitive information (guest kernel memory). (CVE-2023-1859)

Jose Oliveira and Rodrigo Branco discovered that the Spectre Variant 2 mitigations with prctl syscall were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-1998)

It was discovered that the BigBen Interactive Kids' gamepad driver in the Linux kernel did not properly handle device removal, leading to a use- after-free vulnerability. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (system crash). (CVE-2023-25012)

It was discovered that a use-after-free vulnerability existed in the HFS+ file system implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-2985)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6172-1>

Solution

Update the affected kernel package.

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

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-2023-1076 |
| CVE | CVE-2023-1077 |
| CVE | CVE-2023-1079 |
| CVE | CVE-2023-1670 |
| CVE | CVE-2023-1859 |
| CVE | CVE-2023-1998 |
| CVE | CVE-2023-2985 |
| CVE | CVE-2023-25012 |
| XREF | USN:6172-1 |

Plugin Information

Published: 2023/10/23, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-152-generic for this advisory.

168154 - Ubuntu 20.04 LTS / 22.04 LTS : MariaDB vulnerabilities (USN-5739-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5739-1 advisory.

Several security issues were discovered in MariaDB and this update includes new upstream MariaDB versions to fix these issues.

MariaDB has been updated to 10.3.37 in Ubuntu 20.04 LTS and to 10.6.11 in Ubuntu 22.04 LTS and Ubuntu 22.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5739-1>

Solution

Update the affected 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

7.5 (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-2018-25032
CVE CVE-2021-46669
CVE CVE-2022-21427
CVE CVE-2022-27376
CVE CVE-2022-27377
CVE CVE-2022-27378
CVE CVE-2022-27379
CVE CVE-2022-27380
CVE CVE-2022-27381
CVE CVE-2022-27382
CVE CVE-2022-27383
CVE CVE-2022-27384
CVE CVE-2022-27386
CVE CVE-2022-27387
CVE CVE-2022-27444
CVE CVE-2022-27445
CVE CVE-2022-27446
CVE CVE-2022-27447
CVE CVE-2022-27448
CVE CVE-2022-27449
CVE CVE-2022-27451
CVE CVE-2022-27452
CVE CVE-2022-27455
CVE CVE-2022-27456
CVE CVE-2022-27457
CVE CVE-2022-27458
CVE CVE-2022-32081
CVE CVE-2022-32082
CVE CVE-2022-32083
CVE CVE-2022-32084
CVE CVE-2022-32085
CVE CVE-2022-32086
CVE CVE-2022-32087
CVE CVE-2022-32088
CVE CVE-2022-32089
CVE CVE-2022-32091
XREF USN:5739-1

Plugin Information

Published: 2022/11/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.37-0ubuntu0.20.04.1
- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.37-0ubuntu0.20.04.1

189773 - Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6616-1 advisory.

It was discovered that OpenLDAP was not properly performing bounds checks when executing functions related to LDAP URLs. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6616-1>

Solution

Update the affected 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-2023-2953 |
| XREF | USN:6616-1 |

Plugin Information

Published: 2024/01/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.10
- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.10

204858 - Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-6928-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6928-1 advisory.

It was discovered that the Python ssl module contained a memory race condition when handling the APIs to obtain the CA certificates and certificate store

statistics. This could possibly result in applications obtaining wrong results, leading to various SSL issues. (CVE-2024-0397)

It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered private or globally reachable. This could possibly result in applications applying incorrect security policies. (CVE-2024-4032)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6928-1>

Solution

Update the affected 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2024-0397 |
| CVE | CVE-2024-4032 |
| XREF | USN:6928-1 |

Plugin Information

Published: 2024/07/30, Modified: 2024/08/30

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.11
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.11
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.11
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.11
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.11

163679 - Ubuntu 20.04 LTS / 22.04 LTS : Samba vulnerabilities (USN-5542-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5542-1 advisory.

It was discovered that Samba did not handle MaxQueryDuration when being used in AD DC configurations, contrary to expectations. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-3670)

Luke Howard discovered that Samba incorrectly handled certain restrictions associated with changing passwords. A remote attacker being requested to change passwords could possibly use this issue to escalate privileges. (CVE-2022-2031)

Luca Moro discovered that Samba incorrectly handled certain SMB1 communications. A remote attacker could possibly use this issue to obtain sensitive memory contents. (CVE-2022-32742)

Joseph Sutton discovered that Samba incorrectly handled certain password change requests. A remote attacker could use this issue to change passwords of other users, resulting in privilege escalation. (CVE-2022-32744)

Joseph Sutton discovered that Samba incorrectly handled certain LDAP add or modify requests. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-32745)

Joseph Sutton and Andrew Bartlett discovered that Samba incorrectly handled certain LDAP add or modify requests. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-32746)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5542-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-3670 |
| CVE | CVE-2022-2031 |
| CVE | CVE-2022-32742 |
| CVE | CVE-2022-32744 |
| CVE | CVE-2022-32745 |
| CVE | CVE-2022-32746 |
| XREF | USN:5542-1 |
| XREF | IAVA:2022-A-0299-S |

Plugin Information

Published: 2022/08/01, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.13.17~dfsg-0ubuntu1.20.04.1
- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.13.17~dfsg-0ubuntu1.20.04.1
- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.17~dfsg-0ubuntu1.20.04.1

```
- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.17~dfsg-0ubuntu1.20.04.1

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.17~dfsg-0ubuntu1.20.04.1

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.17~dfsg-0ubuntu1.20.04.1

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.17~dfsg-0ubuntu1.20.04.1

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.17~dfsg-0ubuntu1.20.04.1

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.17~dfsg-0ubuntu1.20.04.1
```

207840 - Ubuntu 20.04 LTS / 22.04 LTS : cups-filters vulnerabilities (USN-7043-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7043-1 advisory.

Simone Margaritelli discovered that the cups-filters cups-browsed component could be used to create arbitrary printers from outside the local network. In combination with issues in other printing components, a remote attacker could possibly use this issue to connect to a system, created manipulated PPD files, and execute arbitrary code when a printer is used. This update disables support for the legacy CUPS printer discovery protocol. (CVE-2024-47176)

Simone Margaritelli discovered that cups-filters incorrectly sanitized IPP data when creating PPD files. A remote attacker could possibly use this issue to manipulate PPD files and execute arbitrary code when a printer is used. (CVE-2024-47076)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7043-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.0 (CVSS:3.0/E:F/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

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-47076 |
| CVE | CVE-2024-47176 |
| XREF | USN:7043-1 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/09/27, Modified: 2024/11/25

Plugin Output

tcp/0

```
- Installed package : cups-browsed_1.27.4-1
- Fixed package : cups-browsed_1.27.4-1ubuntu0.3

- Installed package : cups-filters_1.27.4-1
- Fixed package : cups-filters_1.27.4-1ubuntu0.3

- Installed package : cups-filters-core-drivers_1.27.4-1
- Fixed package : cups-filters-core-drivers_1.27.4-1ubuntu0.3

- Installed package : libcupsfilters1_1.27.4-1
- Fixed package : libcupsfilters1_1.27.4-1ubuntu0.3

- Installed package : libfontembed1_1.27.4-1
- Fixed package : libfontembed1_1.27.4-1ubuntu0.3
```

208473 - Ubuntu 20.04 LTS / 22.04 LTS : cups-filters vulnerabilities (USN-7043-4)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7043-4 advisory.

USN-7043-1 fixed vulnerabilities in cups-filters. This update improves the fix for CVE-2024-47176 by removing support for the legacy CUPS printer discovery protocol entirely.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7043-4>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-47076 |
| CVE | CVE-2024-47176 |
| XREF | USN:7043-4 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/10/09, Modified: 2024/11/25

Plugin Output

tcp/0

```
- Installed package : cups-browsed_1.27.4-1
- Fixed package : cups-browsed_1.27.4-1ubuntu0.4

- Installed package : cups-filters_1.27.4-1
- Fixed package : cups-filters_1.27.4-1ubuntu0.4

- Installed package : cups-filters-core-drivers_1.27.4-1
- Fixed package : cups-filters-core-drivers_1.27.4-1ubuntu0.4

- Installed package : libcurlfilters1_1.27.4-1
- Fixed package : libcurlfilters1_1.27.4-1ubuntu0.4

- Installed package : libfontembed1_1.27.4-1
- Fixed package : libfontembed1_1.27.4-1ubuntu0.4
```

155374 - Ubuntu 20.04 LTS : AccountsService vulnerability (USN-5149-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5149-1 advisory.

Kevin Backhouse discovered that AccountsService incorrectly handled memory when performing certain language setting operations. A local attacker could use this issue to escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5149-1>

Solution

Update the affected 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

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-2021-3939 |
| XREF | USN:5149-1 |

Plugin Information

Published: 2021/11/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : accountsservice_0.6.55-0ubuntu12~20.04.1
```

- Fixed package : accountsservice_0.6.55-0ubuntu12~20.04.5
- Installed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.1
- Fixed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.5
- Installed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.1
- Fixed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.5

190715 - Ubuntu 20.04 LTS : Bind vulnerabilities (USN-6642-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6642-1 advisory.

Shoham Danino, Anat Bremler-Barr, Yehuda Afek, and Yuval Shavit discovered that Bind incorrectly handled parsing large DNS messages. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. (CVE-2023-4408)

Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner discovered that Bind incorrectly handled validating DNSSEC messages. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. (CVE-2023-50387)

It was discovered that Bind incorrectly handled preparing an NSEC3 closest encloser proof. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service.

(CVE-2023-50868)

It was discovered that Bind incorrectly handled reverse zone queries when nxdomain-redirect is enabled. A remote attacker could possibly use this issue to cause Bind to crash, leading to a denial of service.

(CVE-2023-5517)

It was discovered that Bind incorrectly handled certain specific recursive query patterns. A remote attacker could possibly use this issue to cause Bind to consume memory, leading to a denial of service.

(CVE-2023-6516)

Bind has been updated to 9.6.48. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://downloads.isc.org/isc/bind9/9.16.48/doc/arm/html/notes.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6642-1>

Solution

Update the affected 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-2023-4408 |
| CVE | CVE-2023-5517 |
| CVE | CVE-2023-6516 |
| CVE | CVE-2023-50387 |
| CVE | CVE-2023-50868 |
| XREF | USN:6642-1 |
| XREF | IAVA:2024-A-0103-S |

Plugin Information

Published: 2024/02/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.48-0ubuntu0.20.04.1
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.48-0ubuntu0.20.04.1
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.48-0ubuntu0.20.04.1

190884 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6649-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6649-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1557)

Alfred Peters discovered that Firefox did not properly manage memory when storing and re-accessing data on a networking channel. An attacker could potentially exploit this issue to cause a denial of service.

(CVE-2024-1546)

Johan Carlsson discovered that Firefox incorrectly handled Set-Cookie response headers in multipart HTTP responses. An attacker could potentially exploit this issue to inject arbitrary cookie values.

(CVE-2024-1551)

Gary Kwong discovered that Firefox incorrectly generated codes on 32-bit ARM devices, which could lead to unexpected numeric conversions or undefined behaviour. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-1552)

Ronald Crane discovered that Firefox did not properly manage memory when accessing the built-in profiler. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1556)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6649-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-1546 |
| CVE | CVE-2024-1547 |
| CVE | CVE-2024-1548 |
| CVE | CVE-2024-1549 |
| CVE | CVE-2024-1550 |
| CVE | CVE-2024-1551 |
| CVE | CVE-2024-1552 |
| CVE | CVE-2024-1553 |
| CVE | CVE-2024-1554 |
| CVE | CVE-2024-1555 |
| CVE | CVE-2024-1556 |
| CVE | CVE-2024-1557 |
| XREF | USN:6649-1 |
| XREF | IAVA:2024-A-0108-S |

Plugin Information

Published: 2024/02/22, Modified: 2025/04/03

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_123.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_123.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_123.0+build3-0ubuntu0.20.04.1

193788 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6747-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6747-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-3852, CVE-2024-3864, CVE-2024-3865)

Bartek Nowotarski discovered that Firefox did not properly limit HTTP/2 CONTINUATION frames. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3302)

Gary Kwong discovered that Firefox did not properly manage memory when running garbage collection during realm initialization. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3853)

Lukas Bernhard discovered that Firefox did not properly manage memory during JIT optimisations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3854, CVE-2024-3855)

Nan Wang discovered that Firefox did not properly manage memory during WASM garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code.
(CVE-2024-3856)

Lukas Bernhard discovered that Firefox did not properly manage memory when handling JIT created code during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3857)

Lukas Bernhard discovered that Firefox did not properly manage memory when tracing in JIT. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3858)

Ronald Crane discovered that Firefox did not properly manage memory in the OpenType sanitizer on 32-bit devices, leading to an out-of-bounds read

vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3859)

Garry Kwong discovered that Firefox did not properly manage memory when tracing empty shape lists in JIT.

An attacker could potentially exploit

this issue to cause a denial of service. (CVE-2024-3860)

Ronald Crane discovered that Firefox did not properly manage memory when handling an AlignedBuffer. An attacker could potentially exploit this

issue to cause denial of service, or execute arbitrary code.

(CVE-2024-3861)

Ronald Crane discovered that Firefox did not properly manage memory when handling code in MarkStack. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

(CVE-2024-3862)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6747-1>

Solution

Update the affected packages.

Risk Factor

High

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

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-2024-3302 |
| CVE | CVE-2024-3852 |
| CVE | CVE-2024-3853 |
| CVE | CVE-2024-3854 |
| CVE | CVE-2024-3855 |
| CVE | CVE-2024-3856 |
| CVE | CVE-2024-3857 |
| CVE | CVE-2024-3858 |
| CVE | CVE-2024-3859 |
| CVE | CVE-2024-3860 |
| CVE | CVE-2024-3861 |
| CVE | CVE-2024-3862 |
| CVE | CVE-2024-3864 |
| CVE | CVE-2024-3865 |
| XREF | USN:6747-1 |
| XREF | IAVA:2024-A-0245-S |

Plugin Information

Published: 2024/04/24, Modified: 2025/04/02

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_125.0.2+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_125.0.2+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_125.0.2+build1-0ubuntu0.20.04.2

147980 - Ubuntu 20.04 LTS : GDK-PixBuf vulnerability (USN-4743-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4743-1 advisory.

It was discovered that the GDK-PixBuf library did not properly handle certain GIF images. If an user or automated system were tricked into opening a specially crafted GIF file, a remote attacker could use this flaw to cause GDK-PixBuf to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4743-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-20240 |
| XREF | USN:4743-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.2
- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.2
- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.2
- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.2

163921 - Ubuntu 20.04 LTS : GDK-PixBuf vulnerability (USN-5554-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5554-1 advisory.

Pedro Ribeiro discovered that the GDK-PixBuf library did not properly handle certain GIF images. If an user or automated system were tricked into opening a specially crafted GIF file, a remote attacker could use this flaw to cause GDK-PixBuf to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5554-1>

Solution

Update the affected 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-2021-46829 |
| XREF | USN:5554-1 |

Plugin Information

Published: 2022/08/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.3

- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.3

- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.3

- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.3
```

140590 - Ubuntu 20.04 LTS : GUPnP vulnerability (USN-4494-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4494-1 advisory.

It was discovered that GUPnP incorrectly handled certain subscription requests. A remote attacker could possibly use this issue to exfiltrate data or use GUPnP to perform DDoS attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4494-1>

Solution

Update the affected gir1.2-gupnp-1.2, libgupnp-1.2-0 and / or libgupnp-1.2-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------------|
| CVE | CVE-2020-12695 |
| XREF | USN:4494-1 |
| XREF | CEA-ID:CEA-2020-0050 |

Plugin Information

Published: 2020/09/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgupnp-1.2-0_1.2.2-1
- Fixed package : libgupnp-1.2-0_1.2.3-0ubuntu0.20.04.1

139312 - Ubuntu 20.04 LTS : Ghostscript vulnerability (USN-4445-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4445-1 advisory.

It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to access arbitrary files, execute arbitrary code,

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4445-1>

Solution

Update the affected 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

8.5 (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-2020-15900 |
| XREF | USN:4445-1 |

Plugin Information

Published: 2020/08/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `ghostscript_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript_9.50~dfsg-5ubuntu4.1`
- Installed package : `ghostscript-x_9.50~dfsg-5ubuntu4`
- Fixed package : `ghostscript-x_9.50~dfsg-5ubuntu4.1`
- Installed package : `libgs9_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9_9.50~dfsg-5ubuntu4.1`
- Installed package : `libgs9-common_9.50~dfsg-5ubuntu4`
- Fixed package : `libgs9-common_9.50~dfsg-5ubuntu4.1`

153211 - Ubuntu 20.04 LTS : Ghostscript vulnerability (USN-5075-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5075-1 advisory.

It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to access arbitrary files, execute arbitrary code, or cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5075-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-3781 |
| XREF | USN:5075-1 |
| XREF | IAVB:2021-B-0055-S |

Plugin Information

Published: 2021/09/10, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.3
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.3
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.3
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.3

152181 - Ubuntu 20.04 LTS : GnuTLS vulnerabilities (USN-5029-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5029-1 advisory.

It was discovered that GnuTLS incorrectly handled sending certain extensions when being used as a client.

A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5029-1>

Solution

Update the affected 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-2021-20231 |
| CVE | CVE-2021-20232 |
| XREF | USN:5029-1 |

Plugin Information

Published: 2021/08/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.6

214007 - Ubuntu 20.04 LTS : HPLIP vulnerability (USN-7202-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7202-1 advisory.

Kevin Backhouse discovered that HPLIP incorrectly handled certain MDNS responses. A remote attacker could use this issue to cause HPLIP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7202-1>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

5.7 (CVSS:3.0:AV:A/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: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-2020-6923 |
| XREF | USN:7202-1 |

Plugin Information

Published: 2025/01/13, Modified: 2025/01/13

Plugin Output

tcp/0

```
- Installed package : hplib_3.20.3+dfsg0-2
- Fixed package : hplib_3.20.3+dfsg0-2ubuntu0.1

- Installed package : hplib-data_3.20.3+dfsg0-2
- Fixed package : hplib-data_3.20.3+dfsg0-2ubuntu0.1

- Installed package : libhpmud0_3.20.3+dfsg0-2
- Fixed package : libhpmud0_3.20.3+dfsg0-2ubuntu0.1

- Installed package : libsane-hpaio_3.20.3+dfsg0-2
- Fixed package : libsane-hpaio_3.20.3+dfsg0-2ubuntu0.1

- Installed package : printer-driver-hpcups_3.20.3+dfsg0-2
- Fixed package : printer-driver-hpcups_3.20.3+dfsg0-2ubuntu0.1

- Installed package : printer-driver-postscript-hp_3.20.3+dfsg0-2
- Fixed package : printer-driver-postscript-hp_3.20.3+dfsg0-2ubuntu0.1
```

181541 - Ubuntu 20.04 LTS : LibRaw vulnerability (USN-6377-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6377-1 advisory.

It was discovered that LibRaw incorrectly handled certain photo files. If a user or automated system were tricked into processing a specially crafted photo file, a remote attacker could possibly cause applications linked against LibRaw to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6377-1>

Solution

Update the affected libraw-bin, libraw-dev and / or libraw19 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-2020-22628 |
| XREF | USN:6377-1 |

Plugin Information

Published: 2023/09/18, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libraw19_0.19.5-1ubuntu1
- Fixed package : libraw19_0.19.5-1ubuntu1.3

165731 - Ubuntu 20.04 LTS : LibreOffice vulnerabilities (USN-5661-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5661-1 advisory.

It was discovered that LibreOffice incorrectly validated macro signatures. If a user were tricked into opening a specially crafted document, a remote attacker could possibly use this issue to execute arbitrary macros. (CVE-2022-26305)

It was discovered that Libreoffice incorrectly handled encrypting the master key provided by the user for storing passwords for web connections. A local attacker could possibly use this issue to obtain access to passwords stored in the user's configuration data. (CVE-2022-26306, CVE-2022-26307)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5661-1>

Solution

Update the affected 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

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-26305 |
| CVE | CVE-2022-26306 |
| CVE | CVE-2022-26307 |
| XREF | USN:5661-1 |
| XREF | IAVB:2022-B-0024-S |

Plugin Information

Published: 2022/10/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.5
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.5

- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-help-en_us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_us_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-l10n-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_gb_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-l10n-en_zh_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_zh_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libbridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libbridl-java_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libuno-purpenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.5
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.5
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.5
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.5

- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.5

158159 - Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5294-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5294-1 advisory.

It was discovered that the Packet network protocol implementation in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-22600)

Szymon Heidrich discovered that the USB Gadget subsystem in the Linux kernel did not properly restrict the size of control requests for certain gadget types, leading to possible out of bounds reads or writes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-39685)

Jann Horn discovered a race condition in the Unix domain socket implementation in the Linux kernel that could result in a read-after-free. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-4083)

Kirill Tkhai discovered that the XFS file system implementation in the Linux kernel did not calculate size correctly when pre-allocating space in some situations. A local attacker could use this to expose sensitive information. (CVE-2021-4155)

Lin Ma discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-4202)

Brendan Dolan-Gavitt discovered that the aQuantia AQtion Ethernet device driver in the Linux kernel did not properly validate meta-data coming from the device. A local attacker who can control an emulated device can use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-43975)

Sushma Venkatesh Reddy discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-0330)

It was discovered that the VMware Virtual GPU driver in the Linux kernel did not properly handle certain failure conditions, leading to a stale entry in the file descriptor table. A local attacker could use this to expose sensitive information or possibly gain administrative privileges. (CVE-2022-22942)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5294-1>

Solution

Update the affected kernel package.

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

7.5 (CVSS:3.0/E:H/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

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

References

| | |
|-----|-------------------------------|
| CVE | CVE-2021-4083 |
| CVE | CVE-2021-4155 |
| CVE | CVE-2021-4202 |

| | |
|------|---------------------------------|
| CVE | CVE-2021-22600 |
| CVE | CVE-2021-39685 |
| CVE | CVE-2021-43975 |
| CVE | CVE-2022-0330 |
| CVE | CVE-2022-22942 |
| XREF | USN:5294-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/05/02 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/02/18, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-100-generic for this advisory.

152555 - Ubuntu 20.04 LTS : MariaDB vulnerabilities (USN-5022-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5022-2 advisory.

USN-5022-1 fixed multiple vulnerabilities in MySQL. This update provides the corresponding fixes for CVE-2021-2372 and CVE-2021-2389 in MariaDB 10.3 and 10.5.

In addition to security fixes, the updated package contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information: <https://mariadb.com/kb/en/mariadb-10331-changelog/> <https://mariadb.com/kb/en/mariadb-10512-changelog/>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5022-2>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|--------------------|
| CVE | CVE-2021-2372 |
| CVE | CVE-2021-2389 |
| XREF | USN:5022-2 |
| XREF | IAVA:2021-A-0333-S |

Plugin Information

Published: 2021/08/13, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.31-0ubuntu0.20.04.1
- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.31-0ubuntu0.20.04.1

139366 - Ubuntu 20.04 LTS : MySQL regression (USN-4441-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4441-2 advisory.

USN-4441-1 fixed vulnerabilities in MySQL. The new upstream version changed compiler options and caused a regression in certain scenarios. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4441-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4441-2

Plugin Information

Published: 2020/08/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.4

183724 - Ubuntu 20.04 LTS : Python vulnerabilities (USN-5201-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5201-1 advisory.

It was discovered that the Python urllib http client could enter into an infinite

loop when incorrectly handling certain server responses (100 Continue response).

Specially crafted traffic from a malicious HTTP server could cause a denial of

service (Dos) condition for a client.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5201-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3737 |
| XREF | USN:5201-1 |

Plugin Information

Published: 2023/10/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.2
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.2
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.2
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.2
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.2

150132 - Ubuntu 20.04 LTS : Python vulnerability (USN-4973-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4973-1 advisory.

It was discovered that the Python stdlib `ipaddress` API incorrectly handled octal strings. A remote attacker could possibly use this issue to perform a wide variety of attacks, including bypassing certain access restrictions.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4973-1>

Solution

Update the affected 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-2021-29921 |
| XREF | USN:4973-1 |

Plugin Information

Published: 2021/06/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `libpython3.8_3.8.2-1ubuntu1.2`
- Fixed package : `libpython3.8_3.8.5-1~20.04.3`
- Installed package : `libpython3.8-minimal_3.8.2-1ubuntu1.2`
- Fixed package : `libpython3.8-minimal_3.8.5-1~20.04.3`
- Installed package : `libpython3.8-stdlib_3.8.2-1ubuntu1.2`
- Fixed package : `libpython3.8-stdlib_3.8.5-1~20.04.3`
- Installed package : `python3.8_3.8.2-1ubuntu1.2`
- Fixed package : `python3.8_3.8.5-1~20.04.3`
- Installed package : `python3.8-minimal_3.8.2-1ubuntu1.2`
- Fixed package : `python3.8-minimal_3.8.5-1~20.04.3`

153852 - Ubuntu 20.04 LTS : Python vulnerability (USN-4973-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4973-2 advisory.

USN-4973-1 fixed this vulnerability previously, but it was re-introduced in python3.8 in focal because of the SRU in LP: #1928057. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4973-2>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-29921 |
| XREF | USN:4973-2 |
| XREF | IAVA:2021-A-0263-S |

Plugin Information

Published: 2021/10/04, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.1

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.1

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.1

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.1

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.1
```

155297 - Ubuntu 20.04 LTS : Samba vulnerabilities (USN-5142-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5142-1 advisory.

Stefan Metzmacher discovered that Samba incorrectly handled SMB1 client connections. A remote attacker could possibly use this issue to downgrade connections to plaintext authentication. (CVE-2016-2124)

Andrew Bartlett discovered that Samba incorrectly mapping domain users to local users. An authenticated attacker could possibly use this issue to become root on domain members. (CVE-2020-25717)

Andrew Bartlett discovered that Samba did not correctly sandbox Kerberos tickets issues by an RODC. An RODC could print administrator tickets, contrary to expectations. (CVE-2020-25718)

Andrew Bartlett discovered that Samba incorrectly handled Kerberos tickets. Delegated administrators could possibly use this issue to impersonate accounts, leading to total domain compromise. (CVE-2020-25719)

Andrew Bartlett discovered that Samba did not provide stable AD identifiers to Kerberos acceptors. (CVE-2020-25721)

Andrew Bartlett discovered that Samba did not properly check sensitive attributes. An authenticated attacker could possibly use this issue to escalate privileges. (CVE-2020-25722)

Stefan Metzmacher discovered that Samba incorrectly handled certain large DCE/RPC requests. A remote attacker could possibly use this issue to bypass signature requirements. (CVE-2021-23192)

William Ross discovered that Samba incorrectly handled memory. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly escalate privileges. (CVE-2021-3738)

Joseph Sutton discovered that Samba incorrectly handled certain TGS requests. An authenticated attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2021-3671)

The fix for CVE-2020-25717 results in possible behaviour changes that could affect certain environments. Please see the upstream advisory for more information:

<https://www.samba.org/samba/security/CVE-2020-25717.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5142-1>

Solution

Update the affected 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

I

References

| | |
|-----|--------------------------------|
| CVE | CVE-2016-2124 |
| CVE | CVE-2020-25717 |
| CVE | CVE-2020-25718 |
| CVE | CVE-2020-25719 |
| CVE | CVE-2020-25721 |
| CVE | CVE-2020-25722 |

| | |
|------|--------------------|
| CVE | CVE-2021-3671 |
| CVE | CVE-2021-3738 |
| CVE | CVE-2021-23192 |
| XREF | USN:5142-1 |
| XREF | IAVA:2021-A-0554-S |

Plugin Information

Published: 2021/11/12, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libsmbclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmbclient_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.14+dfsg-0ubuntu0.20.04.1

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.14+dfsg-0ubuntu0.20.04.1
```

157286 - Ubuntu 20.04 LTS : Samba vulnerabilities (USN-5260-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5260-1 advisory.

Orange Tsai discovered that the Samba vfs_fruit module incorrectly handled certain memory operations. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code as root. (CVE-2021-44142)

Michael Hanselmann discovered that Samba incorrectly created directories. In certain configurations, a remote attacker could possibly create a directory on the server outside of the shared directory.

(CVE-2021-43566)

Kees van Vloten discovered that Samba incorrectly handled certain aliased SPN checks. A remote attacker could possibly use this issue to impersonate services. (CVE-2022-0336)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5260-1>

Solution

Update the affected 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:I/C:A;C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-43566 |
| CVE | CVE-2021-44142 |
| CVE | CVE-2022-0336 |
| XREF | USN:5260-1 |
| XREF | IAVA:2022-A-0054-S |
| XREF | IAVA:2022-A-0020-S |

Plugin Information

Published: 2022/02/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.17~dfsg-0ubuntu0.21.04.1

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.17~dfsg-0ubuntu0.21.04.1
```

157162 - Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5255-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5255-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5255-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-30934 |
| CVE | CVE-2021-30936 |
| CVE | CVE-2021-30951 |
| CVE | CVE-2021-30952 |
| CVE | CVE-2021-30953 |
| CVE | CVE-2021-30954 |
| CVE | CVE-2021-30984 |
| XREF | USN:5255-1 |
| XREF | IAVA:2021-A-0577-S |

Plugin Information

Published: 2022/01/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.34.4-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.34.4-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.34.4-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.34.4-0ubuntu0.20.04.1

150164 - Ubuntu 20.04 LTS : polkit vulnerability (USN-4980-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4980-1 advisory.

Kevin Backhouse discovered that polkit incorrectly handled errors in the polkit_system_bus_name_get_creds_sync function. A local attacker could possibly use this issue to escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4980-1>

Solution

Update the affected 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

7.5 (CVSS:3.0/E:H/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

6.3 (CVSS2#E:H/RL:O/RC:C)

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-3560 |
| XREF | USN:4980-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/06/02 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2021/06/03, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-polkit-1.0_0.105-26ubuntu1
- Fixed package : gir1.2-polkit-1.0_0.105-26ubuntu1.1
- Installed package : libpolkit-agent-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-agent-1-0_0.105-26ubuntu1.1
- Installed package : libpolkit-gobject-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-gobject-1-0_0.105-26ubuntu1.1
- Installed package : policykit-1_0.105-26ubuntu1
- Fixed package : policykit-1_0.105-26ubuntu1.1

57608 - SMB Signing not required**Synopsis**

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

<http://www.nessus.org/u?df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?74b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

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)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)**Synopsis**

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

<https://terrapin-attack.com/>

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```

200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6827-1>

Solution

Update the affected 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-2023-3164 |
| XREF | USN:6827-1 |

Plugin Information

Published: 2024/06/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.13

201111 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6855-1 advisory.

Mansour Gashasbi discovered that libcdio incorrectly handled certain memory operations when parsing an ISO file, leading to a buffer overflow vulnerability. An attacker could use this to cause a denial of service

or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6855-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

6.8 (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-2024-36600 |
| XREF | USN:6855-1 |

Plugin Information

Published: 2024/06/27, Modified: 2025/06/23

Plugin Output

tcp/0

- Installed package : libcdio18_2.0.0-2
- Fixed package : libcdio18_2.0.0-2ubuntu0.2

193701 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerability (USN-6744-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6744-1 advisory.

Hugo van Kemenade discovered that Pillow was not properly performing

bounds checks when processing an ICC file, which could lead to a buffer overflow. If a user or automated system were tricked into processing a specially crafted ICC file, an attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6744-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

CVE-2024-28219
XREF USN:6744-1

Plugin Information

Published: 2024/04/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.9

190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

It was discovered that shadow was not properly sanitizing memory when running the password utility. An attacker could possibly use this issue to retrieve a password from memory, exposing sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6640-1>

Solution

Update the affected 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2023-4641 |
| KREF | USN:6640-1 |

Plugin Information

Published: 2024/02/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : login_1:4.8.1-1ubuntu5.20.04
- Fixed package : login_1:4.8.1-1ubuntu5.20.04.5
- Installed package : passwd_1:4.8.1-1ubuntu5.20.04
- Fixed package : passwd_1:4.8.1-1ubuntu5.20.04.5

240162 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Requests vulnerabilities (USN-7568-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7568-1 advisory.

Dennis Brinkrolf and Tobias Funke discovered that Requests did not correctly handle certain HTTP headers.

A remote attacker could possibly use this issue to leak sensitive information. This issue only affected Ubuntu 14.04 LTS. (CVE-2023-32681)

Juho Forsn discovered that Requests did not correctly parse URLs. A remote attacker could possibly use this issue to leak sensitive information. (CVE-2024-47081)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7568-1>

Solution

Update the affected python-requests, python-requests-whl and / or python3-requests packages.

Risk Factor

Medium

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
CVE CVE-2024-47081
XREF USN:7568-1

Plugin Information

Published: 2025/06/18, Modified: 2025/06/18

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : python3-requests_2.22.0-2ubuntu1
- Fixed package : python3-requests_2.22.0-2ubuntu1.1+esm1

212213 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Expat vulnerability (USN-7145-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7145-1 advisory.

It was discovered that Expat did not properly handle its internal state when attempting to resume an unstarted parser. An attacker could use this issue to cause a denial of service (application crash).

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7145-1>

Solution

Update the affected 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:N/A:H)

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:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-50602 |
| XREF | USN:7145-1 |
| XREF | IAVA:2024-A-0694-S |

Plugin Information

Published: 2024/12/10, Modified: 2025/03/21

Plugin Output

tcp/0

- Installed package : libexpat1_2.2.9-1build1
- Fixed package : libexpat1_2.2.9-1ubuntu0.8

237448 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerability (USN-7542-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7542-1 advisory.

It was discovered that Kerberos allowed the usage of weak cryptographic standards. An attacker could possibly use this issue to expose sensitive information.

This update introduces the allow_rc4 and allow_des3 configuration options, and disables the usage of RC4 and 3DES ciphers by default. Users are advised to discontinue their usage and upgrade to stronger encryption protocols. If the use of the insecure RC4 and 3DES algorithms is necessary, they can be enabled with the aforementioned configuration options.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7542-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2025-3576 |
| XREF | USN:7542-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.11
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.11
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.11
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.11
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.11

206625 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerabilities (USN-6993-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6993-1 advisory.

It was discovered that Vim incorrectly handled memory when closing a window, leading to a double-free vulnerability. If a user was tricked into opening a specially crafted file, an attacker could crash the

application, leading to a denial of service, or possibly achieve code

execution with user privileges. (CVE-2024-41957)

It was discovered that Vim incorrectly handled memory when adding a new file to an argument list, leading to a use-after-free. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service. (CVE-2024-43374)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6993-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-41957 |
| CVE | CVE-2024-43374 |
| XREF | IAVA:2024-A-0461-S |
| XREF | IAVA:2024-A-0505-S |
| XREF | USN:6993-1 |

Plugin Information

Published: 2024/09/05, Modified: 2024/09/05

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.24
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.24
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.24

205112 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : wpa_supplicant and hostapd vulnerability (USN-6945-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6945-1 advisory.

Rory McNamara discovered that wpa_supplicant could be made to load

arbitrary shared objects by unprivileged users that have access to the control interface. An attacker could use this to escalate privileges to root.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6945-1>

Solution

Update the affected 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-2024-5290 |
| XREF | USN:6945-1 |

Plugin Information

Published: 2024/08/06, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : wpasupplicant_2:2.9-1ubuntu4.1
- Fixed package : wpasupplicant_2:2.9-1ubuntu4.4

232662 - Ubuntu 14.04 LTS / 16.04 LTS / 20.04 LTS : Python vulnerabilities (USN-7348-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7348-1 advisory.

It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered private or globally reachable. This could possibly result in applications applying incorrect security policies. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2024-4032)

It was discovered that Python incorrectly handled quoting path names when using the venv module. A local attacker able to control virtual environments could possibly use this issue to execute arbitrary code when the virtual environment is activated. (CVE-2024-9287)

It was discovered that Python incorrectly handled parsing bracketed hosts. A remote attacker could possibly use this issue to perform a Server-Side Request Forgery (SSRF) attack. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2024-11168)

It was discovered that Python incorrectly handled parsing domain names that included square brackets. A remote attacker could possibly use this issue to perform a Server-Side Request Forgery (SSRF) attack.
(CVE-2025-0938)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7348-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

6.3 (CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/V:L/V:A:N/SC:N/SI:L/SA:N)

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:I/C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:O/RC:C)

References

| | |
|-----|----------------|
| CVE | CVE-2024-4032 |
| CVE | CVE-2024-9287 |
| CVE | CVE-2024-11168 |
| CVE | CVE-2025-0938 |

Plugin Information

Published: 2025/03/12, Modified: 2025/03/12

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.16

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.16

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.16

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.16

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.16
```

216423 - Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libsndfile vulnerabilities (USN-7273-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7273-1 advisory.

It was discovered that libsndfile incorrectly handled memory when executing its FLAC codec. If a user or automated system were tricked into processing a specially crafted sound file, an attacker could possibly use this issue to cause a denial of service or obtain sensitive information. (CVE-2021-4156)

It was discovered that libsndfile incorrectly handled certain malformed OggVorbis files. An attacker could possibly use this issue to cause libsndfile to crash, resulting in a denial of service. (CVE-2024-50612)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7273-1>

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

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-2021-4156 |
| CVE | CVE-2024-50612 |
| XREF | USN:7273-1 |

Plugin Information

Published: 2025/02/18, Modified: 2025/02/18

Plugin Output

tcp/0

- Installed package : libsndfile1_1.0.28-7
- Fixed package : libsndfile1_1.0.28-7ubuntu0.3

205444 - Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS : Libcroco vulnerabilities (USN-6958-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6958-1 advisory.

It was discovered that Libcroco was incorrectly accessing data structures when reading bytes from memory, which could cause a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2017-7960)

It was discovered that Libcroco was incorrectly handling invalid UTF-8 values when processing CSS files. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-8834, CVE-2017-8871)

It was discovered that Libcroco was incorrectly implementing recursion in one of its parsing functions, which could cause an infinite recursion loop and a stack overflow due to stack consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-12825)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6958-1>

Solution

Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2017-7960 |
| CVE | CVE-2017-8834 |
| CVE | CVE-2017-8871 |
| CVE | CVE-2020-12825 |
| XREF | USN:6958-1 |

Plugin Information

Published: 2024/08/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcroco3_0.6.13-1
- Fixed package : libcroco3_0.6.13-1ubuntu0.1

186016 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Avahi vulnerabilities (USN-6487-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6487-1 advisory.

Evgeny Vereshchagin discovered that Avahi contained several reachable

assertions, which could lead to intentional assertion failures when

specially crafted user input was given. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-38469, CVE-2023-38470, CVE-2023-38471, CVE-2023-38472, CVE-2023-38473)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6487-1>

Solution

Update the affected 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

4.8 (CVSS:3.0/E:U/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

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

References

| | |
|------|----------------|
| CVE | CVE-2023-38469 |
| CVE | CVE-2023-38470 |
| CVE | CVE-2023-38471 |
| CVE | CVE-2023-38472 |
| CVE | CVE-2023-38473 |
| XREF | USN:6487-1 |

Plugin Information

Published: 2023/11/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : avahi-autoipd_0.7-4ubuntu7
- Fixed package : avahi-autoipd_0.7-4ubuntu7.3
- Installed package : avahi-daemon_0.7-4ubuntu7
- Fixed package : avahi-daemon_0.7-4ubuntu7.3

```
- Installed package : avahi-utils_0.7-4ubuntu7
- Fixed package : avahi-utils_0.7-4ubuntu7.3

- Installed package : libavahi-client3_0.7-4ubuntu7
- Fixed package : libavahi-client3_0.7-4ubuntu7.3

- Installed package : libavahi-common-data_0.7-4ubuntu7
- Fixed package : libavahi-common-data_0.7-4ubuntu7.3

- Installed package : libavahi-common3_0.7-4ubuntu7
- Fixed package : libavahi-common3_0.7-4ubuntu7.3

- Installed package : libavahi-core7_0.7-4ubuntu7
- Fixed package : libavahi-core7_0.7-4ubuntu7.3

- Installed package : libavahi-glib1_0.7-4ubuntu7
- Fixed package : libavahi-glib1_0.7-4ubuntu7.3

- Installed package : libavahi-ui-gtk3-0_0.7-4ubuntu7
- Fixed package : libavahi-ui-gtk3-0_0.7-4ubuntu7.3
```

186644 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : BlueZ vulnerability (USN-6540-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6540-1 advisory.

It was discovered that BlueZ did not properly restrict non-bonded devices from injecting HID events into the input subsystem. This could allow a physically proximate attacker to inject keystrokes and execute arbitrary commands whilst the device is discoverable.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6540-1>

Solution

Update the affected 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 |
| XREF | USN:6540-1 |

Plugin Information

Published: 2023/12/07, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.7

- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.7

- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.7

- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.7
```

185930 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Intel Microcode vulnerability (USN-6485-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6485-1 advisory.

Benoit Morgan, Paul Grosen, Thais Moreira Hamasaki, Ke Sun, Alyssa Milburn, Hisham Shafi, Nir Shlomovich, Tavis Ormandy, Daniel Moghimi, Josh Eads, Salman Qazi, Alexandra Sandulescu, Andy Nguyen, Eduardo Vela, Doug Kwan, and Kostik Shtoyk discovered that some Intel(R) Processors did not properly handle certain sequences of processor instructions. A local attacker could possibly use this to cause a core hang (resulting in a denial of service), gain access to sensitive information or possibly escalate their privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6485-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/U: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:O/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-23583 |
| XREF | USN:6485-1 |

Plugin Information

Published: 2023/11/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20231114.0ubuntu0.20.04.1
```

186991 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6557-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6557-1 advisory.

It was discovered that Vim could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1725)

It was discovered that Vim could be made to recurse infinitely. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1771)

It was discovered that Vim could be made to write out of bounds with a put command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-1886)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1897, CVE-2022-2000)

It was discovered that Vim did not properly manage memory in the spell command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2042)

It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-46246, CVE-2023-48231)

It was discovered that Vim could be made to divide by zero. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-48232)

It was discovered that Vim contained multiple arithmetic overflows. An attacker could possibly use these issues to cause a denial of service. (CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237)

It was discovered that Vim did not properly manage memory in the substitute command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-48706)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6557-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|-----|---------------|
| CVE | CVE-2022-1725 |
| CVE | CVE-2022-1771 |
| CVE | CVE-2022-1886 |

| | |
|------|--------------------|
| CVE | CVE-2022-1897 |
| CVE | CVE-2022-2000 |
| CVE | CVE-2022-2042 |
| CVE | CVE-2023-46246 |
| CVE | CVE-2023-48231 |
| CVE | CVE-2023-48232 |
| CVE | CVE-2023-48233 |
| CVE | CVE-2023-48234 |
| CVE | CVE-2023-48235 |
| CVE | CVE-2023-48236 |
| CVE | CVE-2023-48237 |
| CVE | CVE-2023-48706 |
| XREF | IAVA:2023-A-0598-S |
| XREF | IAVB:2022-B-0049-S |
| XREF | USN:6557-1 |
| XREF | IAVA:2023-A-0650-S |

Plugin Information

Published: 2023/12/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.21
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.21
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.21

178777 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : AMD Microcode vulnerability (USN-6244-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6244-1 advisory.

Tavis Ormandy discovered that some AMD processors did not properly handle speculative execution of certain vector register instructions. A local attacker could use this to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6244-1>

Solution

Update the affected amd64-microcode package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-20593 |
| XREF | USN:6244-1 |

Plugin Information

Published: 2023/07/25, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : amd64-microcode_3.20191218.1ubuntu1
- Fixed package : amd64-microcode_3.20191218.1ubuntu1.1

179940 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Ghostscript vulnerability (USN-6297-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6297-1 advisory.

It was discovered that Ghostscript incorrectly handled outputting certain PDF files. A local attacker could potentially use this issue to cause a crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6297-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-38559 |
| XREF | USN:6297-1 |
| XREF | IAVB:2023-B-0070-S |

Plugin Information

Published: 2023/08/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.9
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.9
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.9
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.9

179733 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Intel Microcode vulnerabilities (USN-6286-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6286-1 advisory.

Daniel Moghimi discovered that some Intel(R) Processors did not properly clear microarchitectural state after speculative execution of various instructions. A local unprivileged user could use this to obtain sensitive information. (CVE-2022-40982)

It was discovered that some Intel(R) Xeon(R) Processors did not properly restrict error injection for Intel(R) SGX or Intel(R) TDX. A local privileged user could use this to further escalate their privileges.

(CVE-2022-41804)

It was discovered that some 3rd Generation Intel(R) Xeon(R) Scalable processors did not properly restrict access in some situations. A local privileged attacker could use this to obtain sensitive information.

(CVE-2023-23908)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6286-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.0 (CVSS:3.0/E:P/R:L/O:RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2022-40982 |
| CVE | CVE-2022-41804 |
| CVE | CVE-2023-23908 |

XREF

USN:6286-1

Plugin Information

Published: 2023/08/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20230808.0ubuntu0.20.04.1

182891 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerability (USN-6428-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6428-1 advisory.

It was discovered that LibTIFF could be made to read out of bounds when processing certain malformed image files with the tiffcrop utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6428-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE
XREF

[CVE-2023-1916](#)
USN:6428-1

Plugin Information

Published: 2023/10/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.10

179306 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6270-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6270-1 advisory.

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2182)

It was discovered that Vim incorrectly handled memory when deleting buffers in diff mode. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2208)

It was discovered that Vim incorrectly handled memory access. An attacker could possibly use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2210)

It was discovered that Vim incorrectly handled memory when using nested :source. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS.

(CVE-2022-2231)

It was discovered that Vim did not properly perform bounds checks when processing a menu item with the only modifier. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2257)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. (CVE-2022-2264, CVE-2022-2284, CVE-2022-2289)

It was discovered that Vim did not properly perform bounds checks when going over the end of the tyahead. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2285)

It was discovered that Vim did not properly perform bounds checks when reading the provided string. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2286)

It was discovered that Vim incorrectly handled memory when adding words with a control character to the internal spell word list. An attacker could possibly use this issue to cause a denial of service.
(CVE-2022-2287)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6270-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-2182 |
| CVE | CVE-2022-2208 |
| CVE | CVE-2022-2210 |
| CVE | CVE-2022-2231 |
| CVE | CVE-2022-2257 |
| CVE | CVE-2022-2264 |
| CVE | CVE-2022-2284 |
| CVE | CVE-2022-2285 |
| CVE | CVE-2022-2286 |
| CVE | CVE-2022-2287 |
| CVE | CVE-2022-2289 |
| XREF | IAVB:2022-B-0049-S |
| XREF | USN:6270-1 |

Plugin Information

Published: 2023/08/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.16

- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.16

- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.16
```

181451 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : gawk vulnerability (USN-6373-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6373-1 advisory.

It was discovered that gawk could be made to read out of bounds when processing certain inputs. If a user or an automated system were tricked into opening a specially crafted input, an attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6373-1>

Solution

Update the affected gawk package.

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

III

References

| | |
|------|------------------|
| CVE | CVE-2023-4156 |
| XREF | IAVA:2023-A-0444 |
| XREF | USN:6373-1 |

Plugin Information

Published: 2023/09/14, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gawk_1:5.0.1+dfsg-1
- Fixed package : gawk_1:5.0.1+dfsg-1ubuntu0.1

180321 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : elfutils vulnerabilities (USN-6322-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6322-1 advisory.

It was discovered that elfutils incorrectly handled certain malformed files. If a user or automated system were tricked into processing a specially crafted file, elfutils could be made to crash or consume resources, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-16062, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7665)

It was discovered that elfutils incorrectly handled bounds checks in certain functions when processing malformed files. If a user or automated system were tricked into processing a specially crafted file, elfutils could be made to crash or consume resources, resulting in a denial of service. (CVE-2020-21047, CVE-2021-33294)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6322-1>

Solution

Update the affected 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

5.9 (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-2018-16062 |
| CVE | CVE-2018-16403 |
| CVE | CVE-2018-18310 |
| CVE | CVE-2018-18520 |
| CVE | CVE-2018-18521 |
| CVE | CVE-2019-7149 |
| CVE | CVE-2019-7150 |

| | |
|------|----------------|
| CVE | CVE-2019-7665 |
| CVE | CVE-2020-21047 |
| CVE | CVE-2021-33294 |
| XREF | USN:6322-1 |

Plugin Information

Published: 2023/08/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libdw1_0.176-1.1build1
- Fixed package : libdw1_0.176-1.1ubuntu0.1
- Installed package : libelf1_0.176-1.1build1
- Fixed package : libelf1_0.176-1.1ubuntu0.1

176745 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : ngnhttp2 vulnerability (USN-6142-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6142-1 advisory.

Gal Goldstein discovered that ngnhttp2 incorrectly handled certain inputs. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6142-1>

Solution

Update the affected 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

6.5 (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)

References

| | |
|------|----------------------|
| CVE | CVE-2020-11080 |
| XREF | USN:6142-1 |
| XREF | CEA-ID:CEA-2021-0004 |

Plugin Information

Published: 2023/06/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnghhttp2-14_1.40.0-1build1
- Fixed package : libnghhttp2-14_1.40.0-1ubuntu0.1

176244 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ncurses vulnerabilities (USN-6099-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6099-1 advisory.

It was discovered that ncurses was incorrectly performing bounds checks when processing invalid hashcodes.

An attacker could possibly use this issue to cause a denial of service or to expose sensitive information.

This issue only affected Ubuntu 18.04 LTS. (CVE-2019-17594)

It was discovered that ncurses was incorrectly handling end-of-string characters when processing terminfo and termcap files. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-17595)

It was discovered that ncurses was incorrectly handling end-of-string characters when converting between termcap and terminfo formats. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-39537)

It was discovered that ncurses was incorrectly performing bounds checks when dealing with corrupt terminfo data while reading a terminfo file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-29458)

It was discovered that ncurses was parsing environment variables when running with setuid applications and not properly handling the processing of malformed data when doing so. A local attacker could possibly use this issue to cause a denial of service (application crash) or execute arbitrary code. (CVE-2023-29491)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6099-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V/C:H/V/I:H/V/A: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-2019-17594 |
| CVE | CVE-2019-17595 |
| CVE | CVE-2021-39537 |
| CVE | CVE-2022-29458 |
| CVE | CVE-2023-29491 |
| XREF | USN:6099-1 |

Plugin Information

Published: 2023/05/23, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : libncurses6_6.2-0ubuntu2
- Fixed package : libncurses6_6.2-0ubuntu2.1
- Installed package : libncursesw6_6.2-0ubuntu2
- Fixed package : libncursesw6_6.2-0ubuntu2.1
- Installed package : libtinfo6_6.2-0ubuntu2
- Fixed package : libtinfo6_6.2-0ubuntu2.1
- Installed package : ncurses-base_6.2-0ubuntu2
- Fixed package : ncurses-base_6.2-0ubuntu2.1
- Installed package : ncurses-bin_6.2-0ubuntu2
- Fixed package : ncurses-bin_6.2-0ubuntu2.1
- Installed package : ncurses-term_6.2-0ubuntu2
- Fixed package : ncurses-term_6.2-0ubuntu2.1

166619 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : DBus vulnerabilities (USN-5704-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5704-1 advisory.

It was discovered that DBus incorrectly handled messages with invalid type signatures. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service. (CVE-2022-42010)

It was discovered that DBus was incorrectly validating the length of arrays of fixed-length items. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service.
(CVE-2022-42011)

It was discovered that DBus incorrectly handled the body DBus message with attached file descriptors. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service.
(CVE-2022-42012)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5704-1>

Solution

Update the affected 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 |
| XREF | USN:5704-1 |

Plugin Information

Published: 2022/10/27, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : dbus_1.12.16-2ubuntu2.1
- Fixed package : dbus_1.12.16-2ubuntu2.3
- Installed package : dbus-user-session_1.12.16-2ubuntu2.1
- Fixed package : dbus-user-session_1.12.16-2ubuntu2.3
- Installed package : dbus-x11_1.12.16-2ubuntu2.1
- Fixed package : dbus-x11_1.12.16-2ubuntu2.3
- Installed package : libdbus-1-3_1.12.16-2ubuntu2.1
- Fixed package : libdbus-1-3_1.12.16-2ubuntu2.3

168452 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU binutils vulnerability (USN-5762-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5762-1 advisory.

It was discovered that GNU binutils incorrectly handled certain

COFF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5762-1>

Solution

Update the affected 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-2022-38533 |
| XREF | USN:5762-1 |

Plugin Information

Published: 2022/12/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.4
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.4
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.4
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.4
- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.4
- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.4

168193 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : JBIG-KIT vulnerability (USN-5742-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5742-1 advisory.

It was discovered that JBIG-KIT incorrectly handled decoding certain large image files. If a user or automated system using JBIG-KIT were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5742-1>

Solution

Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 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

5.9 (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-2017-9937
XREF USN:5742-1

Plugin Information

Published: 2022/11/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libjbig0_2.1-3.1build1
- Fixed package : libjbig0_2.1-3.1ubuntu0.20.04.1

165277 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5619-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5619-1 advisory.

It was discovered that LibTIFF was not properly performing the calculation of data that would eventually be used as a reference for bound-checking operations. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-19131)

It was discovered that LibTIFF was not properly terminating a function execution when processing incorrect data. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-19144)

It was discovered that LibTIFF did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted TIFF file using tiffinfo tool, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-1354)

It was discovered that LibTIFF did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted TIFF file using tiffcp tool, an attacker could possibly use this issue to

cause a denial of service. (CVE-2022-1355)

It was discovered that LibTIFF was not properly performing checks to avoid division calculations where the denominator value was zero, which could lead to an undefined behaviour situation via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2056, CVE-2022-2057, CVE-2022-2058)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5619-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.5 (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:N/A:P)

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2020-19131 |
| CVE | CVE-2020-19144 |
| CVE | CVE-2022-1354 |

| | |
|------|---------------|
| CVE | CVE-2022-1355 |
| CVE | CVE-2022-2056 |
| CVE | CVE-2022-2057 |
| CVE | CVE-2022-2058 |
| XREF | USN:5619-1 |

Plugin Information

Published: 2022/09/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.5

172213 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5923-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5923-1 advisory.

It was discovered that LibTIFF could be made to read out of bounds when processing certain malformed image files with the tiffcrop tool. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service.
(CVE-2023-0795, CVE-2023-0796, CVE-2023-0797, CVE-2023-0798, CVE-2023-0799)

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files with the tiffcrop tool. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2023-0800, CVE-2023-0801, CVE-2023-0802, CVE-2023-0803, CVE-2023-0804)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5923-1>

Solution

Update the affected 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 |
| XREF | USN:5923-1 |

Plugin Information

Published: 2023/03/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.8

166266 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Perl vulnerability (USN-5689-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5689-1 advisory.

It was discovered that Perl incorrectly handled certain signature verification. An remote attacker could possibly use this issue to bypass signature verification.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5689-1>

Solution

Update the affected 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-2020-16156 |
| XREF | USN:5689-1 |

Plugin Information

Published: 2022/10/19, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libperl5.30_5.30.0-9build1
- Fixed package : libperl5.30_5.30.0-9ubuntu0.3
- Installed package : perl_5.30.0-9build1

- Fixed package : perl_5.30.0-9ubuntu0.3
- Installed package : perl-base_5.30.0-9build1
- Fixed package : perl-base_5.30.0-9ubuntu0.3
- Installed package : perl-modules-5.30_5.30.0-9build1
- Fixed package : perl-modules-5.30_5.30.0-9ubuntu0.3

170412 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Setuptools vulnerability (USN-5817-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5817-1 advisory.

Sebastian Chnelik discovered that setuptools incorrectly handled certain regex inputs. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5817-1>

Solution

Update the affected 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:N/A:H)

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:N/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-40897 |
| XREF | USN:5817-1 |

Plugin Information

Published: 2023/01/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pkg-resources_45.2.0-1
- Fixed package : python3-pkg-resources_45.2.0-1ubuntu0.1

171484 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : apr-util vulnerability (USN-5870-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5870-1 advisory.

Ronald Crane discovered that APR-util did not properly handle memory when encoding or decoding certain input data. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5870-1>

Solution

Update the affected 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](#)
XREF USN:5870-1

Plugin Information

Published: 2023/02/15, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libaprutil1_1.6.1-4ubuntu2
- Fixed package : libaprutil1_1.6.1-4ubuntu2.1
- Installed package : libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2
- Fixed package : libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2.1
- Installed package : libaprutil1-ldap_1.6.1-4ubuntu2
- Fixed package : libaprutil1-ldap_1.6.1-4ubuntu2.1

161938 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : e2fsprogs vulnerability (USN-5464-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5464-1 advisory.

Nils Bars discovered that e2fsprogs incorrectly handled certain file systems. A local attacker could use this issue with a crafted file system image to possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5464-1>

Solution

Update the affected 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

6.8 (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-2022-1304 |
| XREF | USN:5464-1 |

Plugin Information

Published: 2022/06/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : e2fsprogs_1.45.5-2ubuntu1
- Fixed package : e2fsprogs_1.45.5-2ubuntu1.1
- Installed package : libcom-err2_1.45.5-2ubuntu1
- Fixed package : libcom-err2_1.45.5-2ubuntu1.1
- Installed package : libext2fs2_1.45.5-2ubuntu1
- Fixed package : libext2fs2_1.45.5-2ubuntu1.1
- Installed package : libss2_1.45.5-2ubuntu1
- Fixed package : libss2_1.45.5-2ubuntu1.1
- Installed package : logsave_1.45.5-2ubuntu1
- Fixed package : logsave_1.45.5-2ubuntu1.1

168316 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : snapd vulnerability (USN-5753-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5753-1 advisory.

The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing the private /tmp mount for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5753-1>

Solution

Update the affected 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

6.0 (CVSS2#AV:L/AC:H/Au:S/C:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE-2022-3328
XREF USN:5753-1

Plugin Information

Published: 2022/12/01, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.57.5+20.04ubuntu0.1

172227 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : systemd vulnerabilities (USN-5928-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5928-1 advisory.

It was discovered that systemd did not properly validate the time and accuracy values provided to the format_timespan() function. An attacker could possibly use this issue to cause a buffer overrun, leading to a denial of service attack. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3821)

It was discovered that systemd did not properly manage the fs.suid_dumpable kernel configurations. A local attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-4415)

It was discovered that systemd did not properly manage a crash with long backtrace data. A local attacker could possibly use this issue to cause a deadlock, leading to a denial of service attack. This issue only affected Ubuntu 22.10. (CVE-2022-45873)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5928-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-3821 |
| CVE | CVE-2022-4415 |
| CVE | CVE-2022-45873 |
| XREF | USN:5928-1 |

Plugin Information

Published: 2023/03/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnss-systemd_245.4-4ubuntu3.2
- Fixed package : libnss-systemd_245.4-4ubuntu3.20
- Installed package : libpam-systemd_245.4-4ubuntu3.2
- Fixed package : libpam-systemd_245.4-4ubuntu3.20
- Installed package : libsystemd0_245.4-4ubuntu3.2
- Fixed package : libsystemd0_245.4-4ubuntu3.20
- Installed package : libudev1_245.4-4ubuntu3.2
- Fixed package : libudev1_245.4-4ubuntu3.20
- Installed package : systemd_245.4-4ubuntu3.2
- Fixed package : systemd_245.4-4ubuntu3.20
- Installed package : systemd-sysv_245.4-4ubuntu3.2
- Fixed package : systemd-sysv_245.4-4ubuntu3.20
- Installed package : systemd-timesyncd_245.4-4ubuntu3.2
- Fixed package : systemd-timesyncd_245.4-4ubuntu3.20
- Installed package : udev_245.4-4ubuntu3.2
- Fixed package : udev_245.4-4ubuntu3.20

172025 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : tar vulnerability (USN-5900-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5900-1 advisory.

It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5900-1>

Solution

Update the affected tar and / or tar-scripts 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-2022-48303
XREF USN:5900-1

Plugin Information

Published: 2023/03/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : tar_1.30+dfsg-7
- Fixed package : tar_1.30+dfsg-7ubuntu0.20.04.3

166103 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : unzip vulnerabilities (USN-5673-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5673-1 advisory.

It was discovered that unzip did not properly handle unicode strings under certain circumstances. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2021-4217)

It was discovered that unzip did not properly perform bounds checking while converting wide strings to local strings. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-0529, CVE-2022-0530)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5673-1>

Solution

Update the affected unzip package.

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-2021-4217 |
| CVE | CVE-2022-0529 |
| CVE | CVE-2022-0530 |
| XREF | USN:5673-1 |

Plugin Information

Published: 2022/10/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : `unzip_6.0-25ubuntu1`
- Fixed package : `unzip_6.0-25ubuntu1.1`

152079 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Aspell vulnerability (USN-5023-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5023-1 advisory.

It was discovered that Aspell incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5023-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2019-25051 |
| XREF | USN:5023-1 |

Plugin Information

Published: 2021/07/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : aspell_0.60.8-1build1
- Fixed package : aspell_0.60.8-1ubuntu0.1
- Installed package : libaspell15_0.60.8-1build1
- Fixed package : libaspell15_0.60.8-1ubuntu0.1

157457 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : BlueZ vulnerability (USN-5275-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5275-1 advisory.

Ziming Zhang discovered that BlueZ incorrectly handled memory write operations in its gatt server. A remote attacker could possibly use this to cause BlueZ to crash leading to a denial of service, or potentially remotely execute code. (CVE-2022-0204)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5275-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2022-0204 |
| XREF | USN:5275-1 |

Plugin Information

Published: 2022/02/09, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.5
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.5
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.5

- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.5

149418 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-4941-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4941-1 advisory.

It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-29457)

It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-29458, CVE-2021-29470)

It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-3482)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4941-1>

Solution

Update the affected 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-2021-3482 |
| CVE | CVE-2021-29457 |
| CVE | CVE-2021-29458 |
| CVE | CVE-2021-29470 |
| XREF | USN:4941-1 |

Plugin Information

Published: 2021/05/12, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libexiv2-27_0.27.2-8ubuntu2
- Fixed package : libexiv2-27_0.27.2-8ubuntu2.2

149906 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-4964-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4964-1 advisory.

It was discovered that Exiv2 incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10 and Ubuntu 21.04.

(CVE-2021-29463)

It was discovered that Exiv2 incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10 and Ubuntu 21.04.

(CVE-2021-29464)

It was discovered that Exiv2 incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-29473, CVE-2021-32617)

It was discovered that Exiv2 incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10 and Ubuntu 21.04.

(CVE-2021-29623)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4964-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-29463 |
| CVE | CVE-2021-29464 |
| CVE | CVE-2021-29473 |
| CVE | CVE-2021-29623 |
| CVE | CVE-2021-32617 |
| XREF | USN:4964-1 |

Plugin Information

Published: 2021/05/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexiv2-27_0.27.2-8ubuntu2
- Fixed package : libexiv2-27_0.27.2-8ubuntu2.4

152637 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-5043-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5043-1 advisory.

It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-32815, CVE-2021-34334, CVE-2021-37620, CVE-2021-37622)

It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. These issues only affected Ubuntu 20.04 LTS and Ubuntu 21.04.

(CVE-2021-34335, CVE-2021-37615, CVE-2021-37616, CVE-2021-37618, CVE-2021-37619, CVE-2021-37621, CVE-2021-37623)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5043-1>

Solution

Update the affected 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

4.3 (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-2021-32815 |
| CVE | CVE-2021-34334 |
| CVE | CVE-2021-34335 |
| CVE | CVE-2021-37615 |
| CVE | CVE-2021-37616 |
| CVE | CVE-2021-37618 |
| CVE | CVE-2021-37619 |
| CVE | CVE-2021-37620 |
| CVE | CVE-2021-37621 |
| CVE | CVE-2021-37622 |
| CVE | CVE-2021-37623 |
| XREF | USN:5043-1 |

Plugin Information

Published: 2021/08/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libexiv2-27_0.27.2-8ubuntu2
- Fixed package : libexiv2-27_0.27.2-8ubuntu2.6

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5672-1 advisory.

It was discovered that GMP did not properly manage memory on 32-bit platforms when processing a specially crafted input. An attacker could possibly use this issue to cause applications using GMP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5672-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2021-43618](#)
XREF USN:5672-1

Plugin Information

Published: 2022/10/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgmp10_2:6.2.0+dfsg-4
- Fixed package : libgmp10_2:6.2.0+dfsg-4ubuntu0.1

152917 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GNOME grilo vulnerability (USN-5055-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5055-1 advisory.

Michael Catanzaro discovered that grilo incorrectly handled certain TLS certificate verification. An attacker could possibly use this issue to MITM attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5055-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

CVE-2021-39365
XREF-USN:5055-1

Plugin Information

Published: 2021/08/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgrilo-0.3-0_0.3.12-1
- Fixed package : libgrilo-0.3-0_0.3.12-1ubuntu0.1

149650 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Base Plugins vulnerability (USN-4959-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4959-1 advisory.

It was discovered that GStreamer Base Plugins incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4959-1>

Solution

Update the affected 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

4.3 (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-2021-3522 |
| XREF | USN:4959-1 |

Plugin Information

Published: 2021/05/18, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-gst-plugins-base-1.0_1.16.2-4
- Fixed package : gir1.2-gst-plugins-base-1.0_1.16.2-4ubuntu0.1
- Installed package : gstreamer1.0-alsa_1.16.2-4
- Fixed package : gstreamer1.0-alsa_1.16.2-4ubuntu0.1
- Installed package : gstreamer1.0-gl_1.16.2-4
- Fixed package : gstreamer1.0-gl_1.16.2-4ubuntu0.1
- Installed package : gstreamer1.0-plugins-base_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base_1.16.2-4ubuntu0.1
- Installed package : gstreamer1.0-plugins-base-apps_1.16.2-4
- Fixed package : gstreamer1.0-plugins-base-apps_1.16.2-4ubuntu0.1
- Installed package : gstreamer1.0-x_1.16.2-4
- Fixed package : gstreamer1.0-x_1.16.2-4ubuntu0.1
- Installed package : libgstreamer-glib1.0-0_1.16.2-4
- Fixed package : libgstreamer-glib1.0-0_1.16.2-4ubuntu0.1
- Installed package : libgstreamer-plugins-base1.0-0_1.16.2-4
- Fixed package : libgstreamer-plugins-base1.0-0_1.16.2-4ubuntu0.1

166109 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5675-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5675-1 advisory.

Isaac Boukris and Andrew Bartlett discovered that Heimdal's KDC was not properly performing checksum algorithm verifications in the S4U2Self extension module. An attacker could possibly use this issue to perform a machine-in-the-middle attack and request S4U2Self tickets for any user known by the application. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2018-16860)

It was discovered that Heimdal was not properly handling the verification of key exchanges when an anonymous PKINIT was being used. An attacker could possibly use this issue to perform a machine-in-the-middle attack and expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2019-12098)

Joseph Sutton discovered that Heimdal was not properly handling memory management operations when dealing with TGS-REQ tickets that were missing information. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-3671)

Micha Kpie discovered that Heimdal was not properly handling logical conditions that related to memory management operations. An attacker could possibly use this issue to cause a denial of service.
(CVE-2022-3116)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5675-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2018-16860 |
| CVE | CVE-2019-12098 |
| CVE | CVE-2021-3671 |
| CVE | CVE-2022-3116 |
| XREF | USN:5675-1 |

Plugin Information

Published: 2022/10/14, Modified: 2025/02/20

Plugin Output

tcp/0

- Installed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libroken18-heimdal_7.7.0+dfsg-1ubuntu1.1
- Installed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1
- Fixed package : libwind0-heimdal_7.7.0+dfsg-1ubuntu1.1

150394 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4985-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4985-1 advisory.

It was discovered that some Intel processors may not properly invalidate cache entries used by Intel Virtualization Technology for Directed I/O (VT-d). This may allow a local user to perform a privilege escalation attack. (CVE-2020-24489)

Joseph Nuzman discovered that some Intel processors may not properly apply EIBRS mitigations (originally developed for CVE-2017-5715) and hence may allow unauthorized memory reads via sidechannel attacks. A local attacker could use this to expose sensitive information, including kernel memory. (CVE-2020-24511)

Travis Downs discovered that some Intel processors did not properly flush cache-lines for trivial-data values. This may allow an unauthorized user to infer the presence of these trivial-data-cache-lines via timing sidechannel attacks. A local attacker could use this to expose sensitive information.
(CVE-2020-24512)

It was discovered that certain Intel Atom processors could expose memory contents stored in microarchitectural buffers. A local attacker could use this to expose sensitive information.
(CVE-2020-24513)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4985-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-24489 |
| CVE | CVE-2020-24511 |
| CVE | CVE-2020-24512 |
| CVE | CVE-2020-24513 |
| XREF | USN:4985-1 |

Plugin Information

Published: 2021/06/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20210608.0ubuntu0.20.04.1

161209 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5421-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5421-1 advisory.

It was discovered that LibTIFF incorrectly handled certain images. An attacker could possibly use this issue to cause a crash, resulting in a denial of service. This issue only affects

Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-35522)

Chintan Shah discovered that LibTIFF incorrectly handled memory when handling certain images. An attacker could possibly use this issue to

cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-0561, CVE-2022-0562, CVE-2022-0891)

It was discovered that LibTIFF incorrectly handled certain images. An attacker could possibly use this issue to cause a crash, resulting in a denial of service. This issue only affects

Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2022-0865)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5421-1>

Solution

Update the affected packages.

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-2020-35522 |
| CVE | CVE-2022-0561 |
| CVE | CVE-2022-0562 |
| CVE | CVE-2022-0865 |
| CVE | CVE-2022-0891 |
| XREF | USN:5421-1 |

Plugin Information

Published: 2022/05/16, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.3
```

174907 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory.

It was discovered that the Traffic-Control Index (TCINDEX) implementation in the Linux kernel did not properly perform filter deactivation in some situations. A local attacker could possibly use this to gain elevated privileges. Please note that with the fix for this CVE, kernel support for the TCINDEX classifier has been removed.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6047-1>

Solution

Update the affected kernel package.

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-2023-1829 |
| XREF | USN:6047-1 |

Plugin Information

Published: 2023/04/27, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-148-generic for this advisory.

159255 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-5342-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5342-1 advisory.

David Schwrer discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-3426)

It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. (CVE-2021-4189)

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-0391)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5342-1>

Solution

Update the affected 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

6.7 (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-2021-3426 |
| CVE | CVE-2021-4189 |
| CVE | CVE-2022-0391 |
| XREF | USN:5342-1 |
| XREF | IAVA:2021-A-0263-S |

Plugin Information

Published: 2022/03/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.4
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.4
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.4
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.4
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.4

157882 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Speex vulnerability (USN-5280-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5280-1 advisory.

It was discovered that Speex incorrectly handled certain WAV files. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5280-1>

Solution

Update the affected 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-2020-23903
XREF USN:5280-1

Plugin Information

Published: 2022/02/10, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libspeex1_1.2~rc1.2-1.1ubuntu1
- Fixed package : libspeex1_1.2~rc1.2-1.1ubuntu1.20.04.1
- Installed package : libspeexdsp1_1.2~rc1.2-1.1ubuntu1
- Fixed package : libspeexdsp1_1.2~rc1.2-1.1ubuntu1.20.04.1

153779 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5093-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5093-1 advisory.

Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-3770)

Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3778)

Dhiraj Mishra discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3796)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5093-1>

Solution

Update the affected 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-2021-3770 |
| CVE | CVE-2021-3778 |
| CVE | CVE-2021-3796 |
| XREF | USN:5093-1 |

Plugin Information

Published: 2021/09/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.3
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.3
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.3

155351 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5147-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5147-1 advisory.

It was discovered that Vim incorrectly handled permissions on the .swp file. A local attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 14.04 ESM.

(CVE-2017-17087)

It was discovered that Vim incorrectly handled restricted mode. A local attacker could possibly use this issue to bypass restricted mode and execute arbitrary commands. Note: This update only makes executing shell commands more difficult. Restricted mode should not be considered a complete security measure. This issue only affected Ubuntu 14.04 ESM. (CVE-2019-20807)

Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 20.04 LTS, Ubuntu 21.04 and Ubuntu 21.10. (CVE-2021-3872)

It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3903)

It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3927)

It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3928)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5147-1>

Solution

Update the affected 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: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

II

References

| | |
|------|--------------------|
| CVE | CVE-2017-17087 |
| CVE | CVE-2019-20807 |
| CVE | CVE-2021-3872 |
| CVE | CVE-2021-3903 |
| CVE | CVE-2021-3927 |
| CVE | CVE-2021-3928 |
| XREF | USN:5147-1 |
| XREF | IAVB:2020-B-0053-S |

Plugin Information

Published: 2021/11/15, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.4
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.4
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.4

154328 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libcaca vulnerabilities (USN-5119-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5119-1 advisory.

It was discovered that libcaca incorrectly handled certain images. An attacker could possibly use this issue to cause a crash. (CVE-2021-30498, CVE-2021-30499)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5119-1>

Solution

Update the affected caca-utils, libcaca-dev and / or libcaca0 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-2021-30498
CVE CVE-2021-30499
XREF USN:5119-1

Plugin Information

Published: 2021/10/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcaca0_0.99.beta19-2.1ubuntu1
- Fixed package : libcaca0_0.99.beta19-2.1ubuntu1.20.04.2

158932 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : tar vulnerability (USN-5329-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5329-1 advisory.

It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to cause tar to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5329-1>

Solution

Update the affected tar and / or tar-scripts 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/V:I:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

2.9 (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-2021-20193 |
| XREF | USN:5329-1 |

Plugin Information

Published: 2022/03/15, Modified: 2024/10/25

Plugin Output

tcp/0

- Installed package : tar_1.30+dfsg-7
- Fixed package : tar_1.30+dfsg-7ubuntu0.20.04.2

200879 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : CUPS vulnerability (USN-6844-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6844-1 advisory.

Rory McNamara discovered that when starting the cupsd server with a Listen configuration item, the cupsd process fails to validate if bind call passed. An attacker could possibly trick cupsd to perform an arbitrary chmod of the provided argument, providing world-writable access to the target.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6844-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-35235 |
| XREF | USN:6844-1 |

Plugin Information

Published: 2024/06/24, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.7

- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.7

- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.7

- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.7

- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.7

- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.7

- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.7

- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.7

- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.7

- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.7

- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.7
```

198069 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6797-1 advisory.

It was discovered that some 3rd and 4th Generation Intel Xeon Processors did not properly restrict access to certain hardware features when using Intel SGX or Intel TDX. This may allow a privileged local user to potentially further escalate their privileges on the system. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-22655)

It was discovered that some Intel Atom Processors did not properly clear register state when performing various operations. A local attacker could use this to obtain sensitive information via a transient execution attack. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-28746)

It was discovered that some Intel Processors did not properly clear the state of various hardware structures when switching execution contexts. A local attacker could use this to access privileged information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-38575)

It was discovered that some Intel Processors did not properly enforce bus lock regulator protections. A remote attacker could use this to cause a denial of service. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-39368)

It was discovered that some Intel Xeon D Processors did not properly calculate the SGX base key when using Intel SGX. A privileged local attacker could use this to obtain sensitive information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-43490)

It was discovered that some Intel Processors did not properly protect against concurrent accesses. A local attacker could use this to obtain sensitive information. (CVE-2023-45733)

It was discovered that some Intel Processors TDX module software did not properly validate input. A privileged local attacker could use this information to potentially further escalate their privileges on the system. (CVE-2023-45745, CVE-2023-47855)

It was discovered that some Intel Core Ultra processors did not properly handle particular instruction sequences. A local attacker could use this issue to cause a denial of service. (CVE-2023-46103)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6797-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-22655 |
| CVE | CVE-2023-28746 |
| CVE | CVE-2023-38575 |
| CVE | CVE-2023-39368 |
| CVE | CVE-2023-43490 |
| CVE | CVE-2023-45733 |
| CVE | CVE-2023-45745 |
| CVE | CVE-2023-46103 |
| CVE | CVE-2023-47855 |
| XREF | USN:6797-1 |

Plugin Information

Published: 2024/05/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20240514.0ubuntu0.20.04.1
```

200257 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : GIFLIB vulnerabilities (USN-6824-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6824-1 advisory.

It was discovered that GIFLIB incorrectly handled certain GIF files. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-40633, CVE-2022-28506, CVE-2023-39742)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6824-1>

Solution

Update the affected giflib-tools, libgif-dev and / or libgif7 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

5.1 (CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.0 (CVSS:2.0/E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-40633 |
| CVE | CVE-2022-28506 |
| CVE | CVE-2023-39742 |
| XREF | USN:6824-1 |

Plugin Information

Published: 2024/06/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgif7_5.1.9-1
- Fixed package : libgif7_5.1.9-1ubuntu0.1

191066 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6664-1 advisory.

It was discovered that less incorrectly handled certain file names. An attacker could possibly use this issue to cause a crash or execute arbitrary commands.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6664-1>

Solution

Update the affected less package.

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:I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-48624 |
| XREF | USN:6664-1 |

Plugin Information

Published: 2024/02/27, Modified: 2025/03/28

Plugin Output

tcp/0

- Installed package : less_551-1ubuntu0.1
- Fixed package : less_551-1ubuntu0.2

237338 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Intel Microcode vulnerabilities (USN-7535-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7535-1 advisory.

Sander Wiebing and Cristiano Giuffrida discovered that some Intel Processors did not properly handle data in Shared Microarchitectural Structures during Transient Execution. An authenticated attacker could possibly use this issue to obtain sensitive information. (CVE-2024-28956)

It was discovered that some Intel Processors did not properly handle prediction calculations. An authenticated attacker could possibly use this issue to obtain sensitive information. (CVE-2024-43420, CVE-2024-45332, CVE-2025-20623)

It was discovered that some Intel Processors did not properly initialize resources in the branch prediction unit. An authenticated attacker could possibly use this issue to obtain sensitive information.

(CVE-2025-20012, CVE-2025-24495)

Michal Raviv and Jeff Gilbert discovered that some Intel Processors did not properly handle resources and exceptions in the core management mechanism. An authenticated attacker could possibly use this issue to cause a denial of service. (CVE-2025-20054, CVE-2025-20103)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7535-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-28956 |
| CVE | CVE-2024-43420 |
| CVE | CVE-2024-45332 |
| CVE | CVE-2025-20012 |
| CVE | CVE-2025-20054 |
| CVE | CVE-2025-20103 |
| CVE | CVE-2025-20623 |
| CVE | CVE-2025-24495 |
| XREF | USN:7535-1 |

Plugin Information

Published: 2025/05/27, Modified: 2025/05/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20250512.0ubuntu0.20.04.1

237450 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libsoup vulnerabilities (USN-7543-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7543-1 advisory.

Jan Raski discovered that libsoup incorrectly handled certain headers when sending HTTP/2 requests over TLS. An attacker could possibly use this issue to cause a denial of service. This issue only affected libsoup3 in Ubuntu 24.04 LTS, Ubuntu 24.10, and Ubuntu 25.04. (CVE-2025-32908)

Jan Raski discovered that libsoup incorrectly parsed certain response headers. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-4476)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7543-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2025-4476 |
| CVE | CVE-2025-32908 |
| XREF | USN:7543-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : gir1.2-soup-2.4_2.70.0-1
- Fixed package : gir1.2-soup-2.4_2.70.0-1ubuntu0.5
- Installed package : libsoup-gnome2.4-1_2.70.0-1
- Fixed package : libsoup-gnome2.4-1_2.70.0-1ubuntu0.5
- Installed package : libsoup2.4-1_2.70.0-1
- Fixed package : libsoup2.4-1_2.70.0-1ubuntu0.5

237727 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libvpx vulnerability (USN-7551-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7551-1 advisory.

It was discovered that libvpx did not properly manage memory. An attacker could possibly use this issue to cause applications using libvpx to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7551-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2025-5283 |
| XREF | USN:7551-1 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : libvpx6_1.8.2-1build1
- Fixed package : libvpx6_1.8.2-1ubuntu0.4

240700 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : urllib3 vulnerabilities (USN-7599-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7599-1 advisory.

Jacob Sandum discovered that urllib3 handled redirects even when they were explicitly disabled while using the PoolManager. An attacker could possibly use this issue to obtain sensitive information.

(CVE-2025-50181)

Illia Volochii discovered that urllib3 incorrectly handled retry and redirect parameters when using Node.js. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 25.04. (CVE-2025-50182)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7599-1>

Solution

Update the affected python-urllib3 and / or python3-urllib3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2025-50181 |
| CVE | CVE-2025-50182 |
| XREF | USN:7599-1 |

Plugin Information

Published: 2025/06/26, Modified: 2025/06/26

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : python3-urllib3_1.25.8-2
- Fixed package : python3-urllib3_1.25.8-2ubuntu0.4+esm1

209342 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : AMD Microcode vulnerability (USN-7077-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has a package installed that is affected by a vulnerability as referenced in the USN-7077-1 advisory.

Enrique Nissim and Krzysztof Okupski discovered that some AMD processors did not properly restrict access to the System Management Mode (SMM) configuration when the SMM Lock was enabled. A privileged local attacker could possibly use this issue to further escalate their privileges and execute arbitrary code within the processor's firmware layer.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7077-1>

Solution

Update the affected amd64-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

5.9 (CVSS:2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.4 (CVSS:2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-31315 |
| XREF | USN:7077-1 |

Plugin Information

Published: 2024/10/21, Modified: 2024/10/21

Plugin Output

tcp/0

- Installed package : amd64-microcode_3.20191218.1ubuntu1
- Fixed package : amd64-microcode_3.20191218.1ubuntu1.3

212270 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7149-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7149-1 advisory.

Avraham Shalev and Nagaraju N Kodalapura discovered that some Intel(R) Xeon(R) processors did not properly restrict access to the memory controller when using Intel(R) SGX. This may allow a local privileged attacker to further escalate their privileges. (CVE-2024-21820, CVE-2024-23918)

It was discovered that some 4th and 5th Generation Intel(R) Xeon(R) Processors did not properly implement finite state machines (FSMs) in hardware logic. THis may allow a local privileged attacker to cause a denial of service (system crash). (CVE-2024-21853)

It was discovered that some Intel(R) Processors did not properly restrict access to the Running Average Power Limit (RAPL) interface. This may allow a local privileged attacker to obtain sensitive information. (CVE-2024-23984)

It was discovered that some Intel(R) Processors did not properly implement finite state machines (FSMs) in hardware logic. This may allow a local privileged attacker to cause a denial of service (system crash). (CVE-2024-24968)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7149-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v4.0 Base Score

8.8 (CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/V/C:H/V/I:H/V/A:H/SC:H/SI:H/SA:H)

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C: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: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-2024-21820 |
| CVE | CVE-2024-21853 |
| CVE | CVE-2024-23918 |
| CVE | CVE-2024-23984 |
| CVE | CVE-2024-24968 |
| XREF | USN:7149-1 |

Plugin Information

Published: 2024/12/11, Modified: 2024/12/11

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20241112.0ubuntu0.20.04.1
```

210284 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenJPEG vulnerabilities (USN-7083-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7083-1 advisory.

It was discovered that OpenJPEG incorrectly handled certain memory operations when using the command line -lImgDir in a directory with a large number of files, leading to an integer overflow vulnerability. An attacker could potentially use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2021-29338)

It was discovered that OpenJPEG incorrectly handled decompressing certain .j2k files in sycc420_to_rgb, leading to a heap-based buffer overflow vulnerability. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to execute arbitrary code. (CVE-2021-3575)

It was discovered that OpenJPEG incorrectly handled certain memory operations in the opj2_decompress program. An attacker could potentially use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-1122)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7083-1>

Solution

Update the affected 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-2021-3575 |
| CVE | CVE-2021-29338 |
| CVE | CVE-2022-1122 |
| XREF | USN:7083-1 |

Plugin Information

Published: 2024/11/05, Modified: 2024/11/05

Plugin Output

tcp/0

- Installed package : libopenjp2-7_2.3.1-1ubuntu4
- Fixed package : libopenjp2-7_2.3.1-1ubuntu4.20.04.3

214505 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenJPEG vulnerabilities (USN-7223-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7223-1 advisory.

Frank Zeng discovered that OpenJPEG incorrectly handled memory when using the decompression utility. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.
(CVE-2024-56826, CVE-2024-56827)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7223-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2024-56826 |
| CVE | CVE-2024-56827 |
| XREF | USN:7223-1 |
| XREF | IAVA:2025-A-0073 |

Plugin Information

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

Plugin Output

tcp/0

- Installed package : libopenjp2-7_2.3.1-1ubuntu4
- Fixed package : libopenjp2-7_2.3.1-1ubuntu4.20.04.4

209876 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : urllib3 vulnerability (USN-7084-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7084-1 advisory.

It was discovered that urllib3 didn't strip HTTP Proxy-Authorization header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7084-1>

Solution

Update the affected python-urllib3 and / or python3-urllib3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-37891 |
| XREF | USN:7084-1 |

Plugin Information

Published: 2024/10/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.25.8-2
- Fixed package : python3-urllib3_1.25.8-2ubuntu0.4

242278 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : libsoup vulnerabilities (USN-7643-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7643-1 advisory.

Jan Raski discovered that libsoup incorrectly handled range headers in an HTTP request. An attacker could possibly use this issue to cause libsoup to consume excessive memory, resulting in a denial of service. (CVE-2025-32907)

Alon Zahavi discovered that libsoup incorrectly handled memory when parsing HTTP requests. An attacker could possibly use this issue to send a maliciously crafted HTTP request to the server, causing a denial of service or obtaining sensitive information. This issue only affected Ubuntu 25.04. (CVE-2025-32914)

It was discovered that libsoup incorrectly handled memory when parsing the expiration date of maliciously crafted cookies. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-4945)

It was discovered that libsoup incorrectly handled integer calculations when parsing multipart data. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-4948)

It was discovered that libsoup incorrectly handled buffer reading when locating boundaries in multipart forms. An attacker could possibly use this issue to cause a denial of service or obtain sensitive information. (CVE-2025-4969)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7643-1>

Solution

Update the affected 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:L/I:N/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:P/I:N/A:P)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:O/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2025-4945 |
| CVE | CVE-2025-4948 |
| CVE | CVE-2025-4969 |
| CVE | CVE-2025-32907 |
| CVE | CVE-2025-32914 |
| XREF | USN:7643-1 |

Plugin Information

Published: 2025/07/17, Modified: 2025/07/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : gir1.2-soup-2.4_2.70.0-1
- Fixed package : gir1.2-soup-2.4_2.70.0-1ubuntu0.5+esm1
- Installed package : libsoup-gnome2.4-1_2.70.0-1
- Fixed package : libsoup-gnome2.4-1_2.70.0-1ubuntu0.5+esm1
- Installed package : libsoup2.4-1_2.70.0-1
- Fixed package : libsoup2.4-1_2.70.0-1ubuntu0.5+esm1

207799 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : APR vulnerability (USN-7038-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7038-1 advisory.

Thomas Stanger discovered a permission vulnerability in the Apache

Portable Runtime (APR) library. A local attacker could possibly use this issue to read named shared memory segments, potentially exposing sensitive application data.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7038-1>

Solution

Update the affected libapr1, libapr1-dev and / or libapr1t64 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-49582 |
| XREF | USN:7038-1 |

Plugin Information

Published: 2024/09/26, Modified: 2024/09/26

Plugin Output

tcp/0

- Installed package : libapr1_1.6.5-1ubuntu1
- Fixed package : libapr1_1.6.5-1ubuntu1.1

205778 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Intel Microcode vulnerabilities (USN-6967-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6967-1 advisory.

It was discovered that some Intel Core Ultra Processors did not properly isolate the stream cache. A local authenticated user could potentially use this to escalate their privileges. (CVE-2023-42667)

It was discovered that some Intel Processors did not properly isolate the stream cache. A local authenticated user could potentially use this to escalate their privileges. (CVE-2023-49141)

It was discovered that some Intel Processors did not correctly transition between the executive monitor and SMI transfer monitor (STM). A privileged local attacker could use this to escalate their privileges.

(CVE-2024-24853)

It was discovered that some 3rd, 4th, and 5th Generation Intel Xeon Processors failed to properly implement a protection mechanism. A local attacker could use this to potentially escalate their privileges. (CVE-2024-24980)

It was discovered that some 3rd Generation Intel Xeon Scalable Processors did not properly handle mirrored regions with different values. A privileged local user could use this to cause a denial of service (system crash). (CVE-2024-25939)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6967-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/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

6.0 (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)

References

| | |
|------|----------------|
| CVE | CVE-2023-42667 |
| CVE | CVE-2023-49141 |
| CVE | CVE-2024-24853 |
| CVE | CVE-2024-24980 |
| CVE | CVE-2024-25939 |
| XREF | USN:6967-1 |

Plugin Information

Published: 2024/08/19, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20240813.0ubuntu0.20.04.2

207801 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJPEG vulnerability (USN-7037-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7037-1 advisory.

It was discovered that OpenJPEG could enter a large loop and continuously print warning messages when given specially crafted input. An attacker could potentially use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7037-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2023-39327](#)
XREF USN:7037-1

Plugin Information

Published: 2024/09/26, Modified: 2024/09/26

Plugin Output

tcp/0

- Installed package : libopenjp2-7_2.3.1-1ubuntu4
- Fixed package : libopenjp2-7_2.3.1-1ubuntu4.20.04.2

209028 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : nano vulnerability (USN-7064-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7064-1 advisory.

It was discovered that nano allowed a possible privilege escalation through an insecure temporary file. If nano was killed while editing, the permissions granted to the emergency save file could be used by an attacker to escalate privileges using a malicious symlink.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7064-1>

Solution

Update the affected nano and / or nano-tiny 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: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 |
| XREF | USN:7064-1 |

Plugin Information

Published: 2024/10/15, Modified: 2024/10/15

Plugin Output

tcp/0

- Installed package : nano_4.8-1ubuntu1
- Fixed package : nano_4.8-1ubuntu1.1

216387 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7269-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7269-1 advisory.

Ke Sun, Paul Gosen and Alyssa Milburn discovered that some Intel Processors did not properly implement Finite State Machines (FSMs) in Hardware Logic. A local privileged attacker could use this issue to cause a denial of service.

(CVE-2024-31068)

It was discovered that some Intel Processors with Intel SGX did not properly restrict access to the EDECCSSA user leaf function. A local authenticated attacker could use this issue to cause a denial of service. (CVE-2024-36293)

Ke Sun, Alyssa Milburn, Benoit Morgan, and Erik Bjorge discovered that the UEFI firmware for some Intel processors did not properly restrict access. An authenticated local attacker could use this issue to cause a denial of service. (CVE-2024-39279)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7269-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v4.0 Base Score

6.8 (CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/V/C:N/V/I:N/V/A:H/SC:N/SI:N/SA:H)

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-31068 |
| CVE | CVE-2024-36293 |
| CVE | CVE-2024-39279 |
| XREF | USN:7269-1 |

Plugin Information

Published: 2025/02/17, Modified: 2025/02/17

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20250211.0ubuntu0.20.04.1

144013 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : APT vulnerability (USN-4667-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4667-1 advisory.

Kevin Backhouse discovered that APT incorrectly handled certain packages. A local attacker could possibly use this issue to cause APT to crash or stop responding, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4667-1>

Solution

Update the affected 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/V/A:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-27350 |
| XREF | USN:4667-1 |

Plugin Information

Published: 2020/12/09, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : apt_2.0.2ubuntu0.1
- Fixed package : apt_2.0.2ubuntu0.2
- Installed package : apt-utils_2.0.2ubuntu0.1
- Fixed package : apt-utils_2.0.2ubuntu0.2
- Installed package : libapt-pkg6.0_2.0.2ubuntu0.1
- Fixed package : libapt-pkg6.0_2.0.2ubuntu0.2

142371 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : AccountsService vulnerabilities (USN-4616-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4616-1 advisory.

Kevin Backhouse discovered that AccountsService incorrectly dropped privileges. A local user could possibly use this issue to cause AccountsService to crash or hang, resulting in a denial of service.

(CVE-2020-16126)

Kevin Backhouse discovered that AccountsService incorrectly handled reading .pam_environment files. A local user could possibly use this issue to cause AccountsService to crash or hang, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2020-16127)

Matthias Gerstner discovered that AccountsService incorrectly handled certain path checks. A local attacker could possibly use this issue to read arbitrary files. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-14036)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4616-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/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

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

References

| | |
|------|----------------|
| BID | 104757 |
| CVE | CVE-2018-14036 |
| CVE | CVE-2020-16126 |
| CVE | CVE-2020-16127 |
| XREF | USN:4616-1 |

Plugin Information

Published: 2020/11/04, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : accountsservice_0.6.55-0ubuntu12~20.04.1
- Fixed package : accountsservice_0.6.55-0ubuntu12~20.04.4

- Installed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.1
- Fixed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.4

- Installed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.1
- Fixed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.4
```

139369 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4449-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4449-1 advisory.

Ryota Shiga working with Trend Micros Zero Day Initiative, discovered that Apport incorrectly dropped privileges when making certain D-Bus calls. A local attacker could use this issue to read arbitrary files.

(CVE-2020-11936)

Seong-Joong Kim discovered that Apport incorrectly parsed configuration files. A local attacker could use this issue to cause Apport to crash, resulting in a denial of service. (CVE-2020-15701)

Ryota Shiga working with Trend Micros Zero Day Initiative, discovered that Apport incorrectly implemented certain checks. A local attacker could use this issue to escalate privileges and run arbitrary code. (CVE-2020-15702)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4449-1>

Solution

Update the affected 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

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)

References

| | |
|------|----------------|
| CVE | CVE-2020-11936 |
| CVE | CVE-2020-15701 |
| CVE | CVE-2020-15702 |
| XREF | USN:4449-1 |

Plugin Information

Published: 2020/08/06, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.6

- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.6

- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.6

- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.6
```

139770 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4468-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4468-1 advisory.

Emanuel Almeida discovered that Bind incorrectly handled certain TCP payloads. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-8620)

Joseph Gullo discovered that Bind incorrectly handled QNAME minimization when used in certain configurations. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-8621)

Dave Feldman, Jeff Warren, and Joel Cunningham discovered that Bind incorrectly handled certain truncated responses to a TSIG-signed request. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2020-8622)

Lyu Chiy discovered that Bind incorrectly handled certain queries. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2020-8623)

Joop Boonen discovered that Bind incorrectly handled certain subdomain update-policy rules. A remote attacker granted privileges to change certain parts of a zone could use this issue to change other contents of the zone, contrary to expectations. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-8624)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4468-1>

Solution

Update the affected 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:N/I:L/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: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-2020-8620 |
| CVE | CVE-2020-8621 |
| CVE | CVE-2020-8622 |
| CVE | CVE-2020-8623 |
| CVE | CVE-2020-8624 |
| XREF | USN:4468-1 |
| XREF | IAVA:2020-A-0385-S |

Plugin Information

Published: 2020/08/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.3
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.3
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.3

149092 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4929-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4929-1 advisory.

Greg Kuechle discovered that Bind incorrectly handled certain incremental zone updates. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2021-25214)

Siva Kakarla discovered that Bind incorrectly handled certain DNAME records. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2021-25215)

It was discovered that Bind incorrectly handled GSSAPI security policy negotiation. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-25216)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4929-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

|

References

| | |
|------|------------------------------------|
| CVE | CVE-2021-25214 |
| CVE | CVE-2021-25215 |
| CVE | CVE-2021-25216 |
| XREF | USN:4929-1 |
| XREF | IAVA:2021-A-0206-S |

Plugin Information

Published: 2021/04/30, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.8
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.8
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.8

148006 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerability (USN-4737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4737-1 advisory.

It was discovered that Bind incorrectly handled GSSAPI security policy negotiation. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly execute arbitrary code. In the default installation, attackers would be isolated by the Bind AppArmor profile.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4737-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2020-8625 |
| XREF | USN:4737-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.6
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.6
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.6

141179 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Brotli vulnerability (USN-4568-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4568-1 advisory.

It was discovered that Brotli incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4568-1>

Solution

Update the affected 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-2020-8927](#)
XREF USN:4568-1

Plugin Information

Published: 2020/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libbrotlii_1.0.7-6build1
- Fixed package : libbrotlii_1.0.7-6ubuntu0.1

140265 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox regressions (USN-4474-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4474-2 advisory.

USN-4474-1 fixed vulnerabilities in Firefox. The update introduced various minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4474-2>

Solution

Update the affected packages.

Risk Factor

Medium

References

XREF USN:4474-2

Plugin Information

Published: 2020/09/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_80.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_80.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_80.0.1+build1-0ubuntu0.20.04.1

139908 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4474-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4474-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, trick the user into installing a malicious extension, spoof the URL bar, leak sensitive information between origins, or execute arbitrary code. (CVE-2020-15664, CVE-2020-15665, CVE-2020-15666, CVE-2020-15670)

It was discovered that NSS incorrectly handled certain signatures. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-12400, CVE-2020-12401, CVE-2020-6829)

A data race was discovered when importing certificate information into the trust store. An attacker could potentially exploit this to cause an unspecified impact. (CVE-2020-15668)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4474-1>

Solution

Update the affected 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

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-2020-12400 |
| CVE | CVE-2020-12401 |
| CVE | CVE-2020-15664 |
| CVE | CVE-2020-15665 |
| CVE | CVE-2020-15666 |
| CVE | CVE-2020-15668 |
| CVE | CVE-2020-15670 |
| CVE | CVE-2020-6829 |
| XREF | USN:4474-1 |
| XREF | IAVA:2020-A-0391-S |

Plugin Information

Published: 2020/08/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_80.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_80.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_80.0+build2-0ubuntu0.20.04.1

140925 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4546-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4546-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, conduct cross-site scripting (XSS) attacks, spoof the site displayed in the download dialog, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4546-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-15673 |
| CVE | CVE-2020-15674 |
| CVE | CVE-2020-15675 |
| CVE | CVE-2020-15676 |
| CVE | CVE-2020-15677 |
| CVE | CVE-2020-15678 |
| XREF | USN:4546-1 |
| XREF | IAVA:2020-A-0435-S |

Plugin Information

Published: 2020/09/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_81.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_81.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_81.0+build2-0ubuntu0.20.04.1

146069 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4717-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4717-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct clickjacking attacks, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4717-1>

Solution

Update the affected 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

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

II

References

| | |
|------|--------------------|
| CVE | CVE-2021-23953 |
| CVE | CVE-2021-23954 |
| CVE | CVE-2021-23955 |
| CVE | CVE-2021-23956 |
| CVE | CVE-2021-23958 |
| CVE | CVE-2021-23960 |
| CVE | CVE-2021-23961 |
| CVE | CVE-2021-23962 |
| CVE | CVE-2021-23963 |
| CVE | CVE-2021-23964 |
| CVE | CVE-2021-23965 |
| XREF | USN:4717-1 |
| XREF | IAVA:2021-A-0185-S |

Plugin Information

Published: 2021/02/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_85.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_85.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_85.0+build1-0ubuntu0.20.04.1

147994 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4756-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4756-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct cross-site scripting (XSS) attacks, bypass HTTP auth phishing warnings, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4756-1>

Solution

Update the affected 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

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-2021-23968 |
| CVE | CVE-2021-23969 |
| CVE | CVE-2021-23970 |
| CVE | CVE-2021-23971 |
| CVE | CVE-2021-23972 |
| CVE | CVE-2021-23973 |
| CVE | CVE-2021-23974 |
| CVE | CVE-2021-23975 |
| CVE | CVE-2021-23978 |
| CVE | CVE-2021-23979 |
| XREF | USN:4756-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_86.0+build3-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_86.0+build3-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_86.0+build3-0ubuntu0.20.04.1
```

148135 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4893-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4893-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2021-23981, CVE-2021-23982, CVE-2021-23983, CVE-2021-23987, CVE-2021-

23988)

It was discovered that extensions could open popup windows with control of the window title in some circumstances. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to spook a website and trick the user into providing credentials. (CVE-2021-23984)

It was discovered that the DevTools remote debugging feature could be enabled without an indication to the user. If a local attacker could modify the browser configuration, a remote attacker could potentially exploit this to obtain sensitive information. (CVE-2021-23985)

It was discovered that extensions could read the response of cross origin requests in some circumstances.

If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to obtain sensitive information. (CVE-2021-23986)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4893-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-23981 |
| CVE | CVE-2021-23982 |
| CVE | CVE-2021-23983 |
| CVE | CVE-2021-23984 |
| CVE | CVE-2021-23985 |
| CVE | CVE-2021-23986 |
| CVE | CVE-2021-23987 |
| CVE | CVE-2021-23988 |
| XREF | IAVA:2021-A-0144-S |
| XREF | USN:4893-1 |

Plugin Information

Published: 2021/03/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_87.0+build3-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_87.0+build3-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_87.0+build3-0ubuntu0.20.04.2

148992 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4926-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4926-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, trick the user into disclosing confidential information, or execute arbitrary code. (CVE-2021-23994, CVE-2021-23996, CVE-2021-23997, CVE-2021-23998, CVE-2021-23999, CVE-2021-24000, CVE-2021-24001, CVE-2021-29945, CVE-2021-29946, CVE-2021-29947)

A use-after-free was discovered when Responsive Design Mode was enabled. If a user were tricked into opening a specially crafted website with Responsive Design Mode enabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2021-23995)

It was discovered that Firefox mishandled ftp URLs with encoded newline characters. If a user were tricked into clicking on a specially crafted link, an attacker could potentially exploit this to send arbitrary FTP commands. (CVE-2021-24002)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4926-1>

Solution

Update the affected 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

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-2021-23994 |
| CVE | CVE-2021-23995 |
| CVE | CVE-2021-23996 |
| CVE | CVE-2021-23997 |
| CVE | CVE-2021-23998 |
| CVE | CVE-2021-23999 |
| CVE | CVE-2021-24000 |
| CVE | CVE-2021-24001 |
| CVE | CVE-2021-24002 |
| CVE | CVE-2021-29945 |
| CVE | CVE-2021-29946 |
| CVE | CVE-2021-29947 |
| XREF | USN:4926-1 |

Plugin Information

Published: 2021/04/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_88.0+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_88.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_88.0+build2-0ubuntu0.20.04.1

144808 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerability (USN-4687-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4687-1 advisory.

A use-after-free was discovered in Firefox when handling SCTP packets. An attacker could potentially exploit this to cause a denial of service, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4687-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2020-16044 |
| XREF | USN:4687-1 |
| XREF | IAVA:2021-A-0005-S |

Plugin Information

Published: 2021/01/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_84.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_84.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_84.0.2+build1-0ubuntu0.20.04.1

141615 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : FreeType vulnerability (USN-4593-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4593-1 advisory.

Sergei Glazunov discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4593-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:H/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

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

References

| | |
|------|---|
| CVE | CVE-2020-15999 |
| XREF | USN:4593-1 |
| XREF | CISA-KNOWN-EXPLOITED:2021/11/17 |
| XREF | CEA-ID:CEA-2020-0124 |

Plugin Information

Published: 2020/10/20, Modified: 2025/02/07

Plugin Output

tcp/0

- Installed package : libfreetype6_2.10.1-2
- Fixed package : libfreetype6_2.10.1-2ubuntu0.1

147993 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GLib vulnerabilities (USN-4759-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4759-1 advisory.

Krzesimir Nowak discovered that GLib incorrectly handled certain large buffers. A remote attacker could use this issue to cause applications linked to GLib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-27218)

Kevin Backhouse discovered that GLib incorrectly handled certain memory allocations. A remote attacker could use this issue to cause applications linked to GLib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-27219)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4759-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-27218 |
| CVE | CVE-2021-27219 |
| XREF | USN:4759-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.2
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.2
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.2

147989 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GLib vulnerability (USN-4764-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4764-1 advisory.

It was discovered that GLib incorrectly handled certain symlinks when replacing files. If a user or automated system were tricked into extracting a specially crafted file with File Roller, a remote attacker could possibly create files outside of the intended directory.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4764-1>

Solution

Update the affected 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-2021-28153 |
| XREF | USN:4764-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.3
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.3
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.3

139179 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GRUB 2 vulnerabilities (USN-4432-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4432-1 advisory.

Jesse Michael and Mickey Shkatov discovered that the configuration parser in GRUB2 did not properly exit when errors were discovered, resulting in heap-based buffer overflows. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. (CVE-2020-10713)

Chris Coulson discovered that the GRUB2 function handling code did not properly handle a function being redefined, leading to a use-after-free vulnerability. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. (CVE-2020-15706)

Chris Coulson discovered that multiple integer overflows existed in GRUB2 when handling certain filesystems or font files, leading to heap-based buffer overflows. A local attacker could use these to execute arbitrary code and bypass UEFI Secure Boot restrictions. (CVE-2020-14309, CVE-2020-14310, CVE-2020-14311)

It was discovered that the memory allocator for GRUB2 did not validate allocation size, resulting in multiple integer overflows and heap-based buffer overflows when handling certain filesystems, PNG images or disk metadata. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. (CVE-2020-14308)

Mathieu Trudel-Lapierre discovered that in certain situations, GRUB2 failed to validate kernel signatures. A local attacker could use this to bypass Secure Boot restrictions. (CVE-2020-15705)

Colin Watson and Chris Coulson discovered that an integer overflow existed in GRUB2 when handling the initrd command, leading to a heap-based buffer overflow. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. (CVE-2020-15707)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4432-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|----------------------|
| CVE | CVE-2020-10713 |
| CVE | CVE-2020-14308 |
| CVE | CVE-2020-14309 |
| CVE | CVE-2020-14310 |
| CVE | CVE-2020-14311 |
| CVE | CVE-2020-15705 |
| CVE | CVE-2020-15706 |
| CVE | CVE-2020-15707 |
| XREF | USN:4432-1 |
| XREF | IAVA:2020-A-0349 |
| XREF | CEA-ID:CEA-2020-0061 |

Plugin Information

Published: 2020/07/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : grub-common_2.04-1ubuntu26
- Fixed package : grub-common_2.04-1ubuntu26.1
- Installed package : grub-pc_2.04-1ubuntu26
- Fixed package : grub-pc_2.04-1ubuntu26.1
- Installed package : grub-pc-bin_2.04-1ubuntu26
- Fixed package : grub-pc-bin_2.04-1ubuntu26.1
- Installed package : grub2-common_2.04-1ubuntu26
- Fixed package : grub2-common_2.04-1ubuntu26.1

139365 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GRUB2 regression (USN-4432-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4432-2 advisory.

USN-4432-1 fixed vulnerabilities in GRUB2 affecting Secure Boot environments. Unfortunately, the update introduced regressions for some BIOS systems (either

pre-UEFI or UEFI configured in Legacy mode), preventing them from successfully booting. This update addresses the issue.

Users with BIOS systems that installed GRUB2 versions from USN-4432-1 should verify that their GRUB2 installation has a correct understanding of their boot device location and installed the boot loader correctly.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4432-2>

Solution

Update the affected packages.

Risk Factor

Medium

STIG Severity

II

References

XREF USN:4432-2
XREF IAVA:2020-A-0349

Plugin Information

Published: 2020/08/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : grub-common_2.04-1ubuntu26
- Fixed package : grub-common_2.04-1ubuntu26.2
- Installed package : grub-pc_2.04-1ubuntu26
- Fixed package : grub-pc_2.04-1ubuntu26.2
- Installed package : grub-pc-bin_2.04-1ubuntu26
- Fixed package : grub-pc-bin_2.04-1ubuntu26.2
- Installed package : grub2-common_2.04-1ubuntu26
- Fixed package : grub2-common_2.04-1ubuntu26.2

149055 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-4928-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4928-1 advisory.

It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to cause access sensitive information or cause a crash. (CVE-2021-3497)

It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code or cause a crash. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-3498)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4928-1>

Solution

Update the affected 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-2021-3497 |
| CVE | CVE-2021-3498 |
| XREF | USN:4928-1 |

Plugin Information

Published: 2021/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gstreamer1.0-gtk3_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-gtk3_1.16.2-1ubuntu2.1
- Installed package : gstreamer1.0-plugins-good_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-plugins-good_1.16.2-1ubuntu2.1
- Installed package : gstreamer1.0-pulseaudio_1.16.2-1ubuntu2
- Fixed package : gstreamer1.0-pulseaudio_1.16.2-1ubuntu2.1
- Installed package : libgstreamer-plugins-good1.0-0_1.16.2-1ubuntu2
- Fixed package : libgstreamer-plugins-good1.0-0_1.16.2-1ubuntu2.1

139782 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-4469-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4469-1 advisory.

It was discovered that Ghostscript incorrectly handled certain document files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4469-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-16287 |
| CVE | CVE-2020-16288 |
| CVE | CVE-2020-16289 |
| CVE | CVE-2020-16290 |
| CVE | CVE-2020-16291 |
| CVE | CVE-2020-16292 |
| CVE | CVE-2020-16293 |
| CVE | CVE-2020-16294 |
| CVE | CVE-2020-16295 |
| CVE | CVE-2020-16296 |
| CVE | CVE-2020-16297 |
| CVE | CVE-2020-16298 |
| CVE | CVE-2020-16299 |
| CVE | CVE-2020-16300 |
| CVE | CVE-2020-16301 |
| CVE | CVE-2020-16302 |
| CVE | CVE-2020-16303 |
| CVE | CVE-2020-16304 |
| CVE | CVE-2020-16305 |
| CVE | CVE-2020-16306 |
| CVE | CVE-2020-16307 |
| CVE | CVE-2020-16308 |
| CVE | CVE-2020-16309 |
| CVE | CVE-2020-16310 |
| CVE | CVE-2020-17538 |
| XREF | USN:4469-1 |
| XREF | IAVB:2020-B-0046-S |

Plugin Information

Published: 2020/08/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.2
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.2
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.2
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.2

142967 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Kerberos vulnerability (USN-4635-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4635-1 advisory.

Demi Obenour discovered that Kerberos incorrectly handled certain ASN.1. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4635-1>

Solution

Update the affected 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

6.5 (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)

References

| | |
|------|--------------------------------------|
| CVE | CVE-2020-28196 |
| XREF | USN:4635-1 |
| XREF | CEA-ID:CEA-2021-0025 |

Plugin Information

Published: 2020/11/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.1
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.1
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.1
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.1
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.1

148000 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-4755-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4755-1 advisory.

It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4755-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-35523 |
| CVE | CVE-2020-35524 |
| XREF | USN:4755-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.1

142998 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer, Vino vulnerability (USN-4636-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4636-1 advisory.

It was discovered that LibVNCServer incorrectly handled certain internals. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Vino package ships with a LibVNCServer source and all listed releases were affected for this package.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4636-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-25708 |
| XREF | USN:4636-1 |

Plugin Information

Published: 2020/11/18, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libvncclient1_0.9.12+dfsg-9ubuntu0.2
- Fixed package : libvncclient1_0.9.12+dfsg-9ubuntu0.3
- Installed package : vino_3.22.0-5ubuntu2
- Fixed package : vino_3.22.0-5ubuntu2.2

141541 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4591-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4591-1 advisory.

Andy Nguyen discovered that the Bluetooth L2CAP implementation in the Linux kernel contained a type- confusion error. A physically proximate remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-12351)

Andy Nguyen discovered that the Bluetooth A2MP implementation in the Linux kernel did not properly initialize memory in some situations. A physically proximate remote attacker could use this to expose sensitive information (kernel memory). (CVE-2020-12352)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4591-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-12351 |
| CVE | CVE-2020-12352 |
| XREF | USN:4591-1 |

Plugin Information

Published: 2020/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-52-generic for this advisory.

145007 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4694-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4694-1 advisory.

It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4694-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

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

7.1 (CVSS:3.0/E:U/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

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

References

| | |
|------|----------------|
| CVE | CVE-2020-28374 |
| XREF | USN:4694-1 |

Plugin Information

Published: 2021/01/14, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-62-generic for this advisory.

139480 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerabilities (USN-4455-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4455-1 advisory.

It was discovered that NSS incorrectly handled certain signatures. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-12400, CVE-2020-12401, CVE-2020-6829)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4455-1>

Solution

Update the affected 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:L/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-12400 |
| CVE | CVE-2020-12401 |
| CVE | CVE-2020-6829 |
| XREF | USN:4455-1 |

Plugin Information

Published: 2020/08/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.4

140030 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-4476-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4476-1 advisory.

It was discovered that NSS incorrectly handled some inputs. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4476-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-12403 |
| XREF | USN:4476-1 |

Plugin Information

Published: 2020/08/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.5

148491 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Nettle vulnerability (USN-4906-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4906-1 advisory.

It was discovered that Nettle incorrectly handled signature verification. A remote attacker could use this issue to cause Nettle to crash, resulting in a denial of service, or possibly force invalid signatures.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4906-1>

Solution

Update the affected packages.

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-2021-20305
XREF USN:4906-1

Plugin Information

Published: 2021/04/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libhogweed5_3.5.1+really3.5.1-2
- Fixed package : libhogweed5_3.5.1+really3.5.1-2ubuntu0.1

- Installed package : libnettle7_3.5.1+really3.5.1-2
- Fixed package : libnettle7_3.5.1+really3.5.1-2ubuntu0.1

142966 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerabilities (USN-4634-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4634-1 advisory.

It was discovered that OpenLDAP incorrectly handled certain malformed inputs. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4634-1>

Solution

Update the affected 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

6.5 (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)

References

| | |
|------|----------------|
| CVE | CVE-2020-25709 |
| CVE | CVE-2020-25710 |
| XREF | USN:4634-1 |

Plugin Information

Published: 2020/11/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.5
- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.5

146302 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerabilities (USN-4724-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4724-1 advisory.

It was discovered that OpenLDAP incorrectly handled Certificate Exact Assertion processing. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service.

(CVE-2020-36221)

It was discovered that OpenLDAP incorrectly handled saslAuthzTo processing. A remote attacker could use this issue to cause OpenLDAP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-36222, CVE-2020-36224, CVE-2020-36225, CVE-2020-36226)

It was discovered that OpenLDAP incorrectly handled Return Filter control handling. A remote attacker could use this issue to cause OpenLDAP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-36223)

It was discovered that OpenLDAP incorrectly handled certain cancel operations. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service. (CVE-2020-36227)

It was discovered that OpenLDAP incorrectly handled Certificate List Extract Assertion processing. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service. (CVE-2020-36228)

It was discovered that OpenLDAP incorrectly handled X.509 DN parsing. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service. (CVE-2020-36229, CVE-2020-36230)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4724-1>

Solution

Update the affected 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

6.5 (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-2020-36221 |
| CVE | CVE-2020-36222 |
| CVE | CVE-2020-36223 |
| CVE | CVE-2020-36224 |
| CVE | CVE-2020-36225 |
| CVE | CVE-2020-36226 |
| CVE | CVE-2020-36227 |
| CVE | CVE-2020-36228 |
| CVE | CVE-2020-36229 |
| CVE | CVE-2020-36230 |
| XREF | USN:4724-1 |
| XREF | IAVB:2021-B-0014 |

Plugin Information

Published: 2021/02/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.6
- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.6

142735 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4622-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4622-1 advisory.

It was discovered that OpenLDAP incorrectly handled certain network packets. A remote attacker could use this issue to cause OpenLDAP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4622-1>

Solution

Update the affected 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

6.5 (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)

References

| | |
|------|----------------|
| CVE | CVE-2020-25692 |
| XREF | USN:4622-1 |

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.4
- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.4

147986 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4744-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4744-1 advisory.

Pasi Saarinen discovered that OpenLDAP incorrectly handled certain short timestamps. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4744-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-27212 |
| XREF | USN:4744-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-2.4-2_2.4.49+dfsg-2ubuntu1.7
- Installed package : libldap-common_2.4.49+dfsg-2ubuntu1.3
- Fixed package : libldap-common_2.4.49+dfsg-2ubuntu1.7

143428 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PEAR vulnerabilities (USN-4654-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4654-1 advisory.

It was discovered that PEAR incorrectly sanitized filenames. A remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4654-1>

Solution

Update the affected php-pear package.

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

7.2 (CVSS:3.0/E:F/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

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2020-28948 |
| CVE | CVE-2020-28949 |
| XREF | USN:4654-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/09/15 |

Exploitable With

Metasploit (true)

Plugin Information

Published: 2020/12/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : php-pear_1:1.10.9+submodules+notgz-1
- Fixed package : php-pear_1:1.10.9+submodules+notgz-1ubuntu0.20.04.1

146301 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PEAR vulnerability (USN-4723-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4723-1 advisory.

It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4723-1>

Solution

Update the affected php-pear package.

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

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:P/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2020-36193 |
| XREF | USN:4723-1 |
| XREF | CISA-KNOWN-EXPLOITED:2022/09/15 |

Plugin Information

Published: 2021/02/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : php-pear_1:1.10.9+submodules+notgz-1
- Fixed package : php-pear_1:1.10.9+submodules+notgz-1ubuntu0.20.04.2

145048 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-4697-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4697-1 advisory.

It was discovered that Pillow incorrectly handled certain PCX image files. If a user or automated system were tricked into opening a specially-crafted PCX file, a remote attacker could possibly cause Pillow to crash, resulting in a denial of service. (CVE-2020-35653)

It was discovered that Pillow incorrectly handled certain Tiff image files. If a user or automated system were tricked into opening a specially-crafted Tiff file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2020-35654)

It was discovered that Pillow incorrectly handled certain SGI image files. If a user or automated system were tricked into opening a specially-crafted SGI file, a remote attacker could possibly cause Pillow to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2020-35655)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4697-1>

Solution

Update the affected 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-2020-35653 |
| CVE | CVE-2020-35654 |
| CVE | CVE-2020-35655 |
| XREF | USN:4697-1 |

Plugin Information

Published: 2021/01/18, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.2

147969 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pygments vulnerability (USN-4885-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4885-1 advisory.

It was discovered that Pygments incorrectly handled parsing SML files. If a user or automated system were tricked into parsing a specially crafted SML file, a

remote attacker could cause Pygments to hang, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4885-1>

Solution

Update the affected python-pygments and / or python3-pygments 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

6.5 (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)

References

CVE-2021-20270
XREF USN:4885-1

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pygments_2.3.1+dfsg-1ubuntu2
- Fixed package : python3-pygments_2.3.1+dfsg-1ubuntu2.1

148248 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pygments vulnerability (USN-4897-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4897-1 advisory.

Ben Caller discovered that Pygments incorrectly handled parsing certain files. If a user or automated system were tricked into parsing a specially crafted file, a remote attacker could cause Pygments to hang or consume resources, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4897-1>

Solution

Update the affected python-pygments and / or python3-pygments 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

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

CVSS v2.0 Temporal Score

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

References

CVE-2021-27291
USN:4897-1

Plugin Information

Published: 2021/03/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pgments_2.3.1+dfsg-1ubuntu2
- Fixed package : python3-pgments_2.3.1+dfsg-1ubuntu2.2

142739 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Raptor vulnerability (USN-4630-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4630-1 advisory.

Hanno Bck discovered that Raptor incorrectly handled certain memory operations. If a user were tricked into opening a specially crafted document in an application linked against Raptor, an attacker could cause the application to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4630-1>

Solution

Update the affected libraptor2-0, libraptor2-dev and / or raptor2-utils packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2017-18926 |
| XREF | USN:4630-1 |

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libraptor2-0_2.0.15-0ubuntu1
- Fixed package : libraptor2-0_2.0.15-0ubuntu1.20.04.1

142218 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerabilities (USN-4611-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4611-1 advisory.

Steven French discovered that Samba incorrectly handled ChangeNotify permissions. A remote attacker could possibly use this issue to obtain file name information. (CVE-2020-14318)

Bas Alberts discovered that Samba incorrectly handled certain winbind requests. A remote attacker could possibly use this issue to cause winbind to crash, resulting in a denial of service. (CVE-2020-14323)

Francis Brosnan Blzquez discovered that Samba incorrectly handled certain invalid DNS records. A remote attacker could possibly use this issue to cause the DNS server to crash, resulting in a denial of service.

(CVE-2020-14383)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4611-1>

Solution

Update the affected 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 (CVSS:2#AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS:2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2020-14318 |
| CVE | CVE-2020-14323 |
| CVE | CVE-2020-14383 |
| XREF | USN:4611-1 |

Plugin Information

Published: 2020/11/02, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.6

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.6
```

139479 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4454-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4454-1 advisory.

Martin von Wittich and Wilko Meyer discovered that Samba incorrectly handled certain empty UDP packets when being used as a AD DC NBT server. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4454-1>

Solution

Update the affected 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

6.5 (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)

References

CVE-2020-14303
XREF USN:4454-1

Plugin Information

Published: 2020/08/11, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.4

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.4
```

149093 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4930-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4930-1 advisory.

Peter Eriksson discovered that Samba incorrectly handled certain negative idmap cache entries. This issue could result in certain users gaining unauthorized access to files, contrary to expected behaviour.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4930-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-20254 |
| XREF | USN:4930-1 |
| XREF | IAVA:2021-A-0208-S |

Plugin Information

Published: 2021/04/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.8
- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.8

139370 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Whoopsie vulnerabilities (USN-4450-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4450-1 advisory.

Seong-Joong Kim discovered that Whoopsie incorrectly handled memory. A local attacker could use this issue to cause Whoopsie to consume memory, resulting in a denial of service. (CVE-2020-11937)

Seong-Joong Kim discovered that Whoopsie incorrectly handled parsing files. A local attacker could use this issue to cause Whoopsie to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-12135)

Seong-Joong Kim discovered that Whoopsie incorrectly handled memory. A local attacker could use this issue to cause Whoopsie to consume memory, resulting in a denial of service. (CVE-2020-15570)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4450-1>

Solution

Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie 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-2020-11937 |
| CVE | CVE-2020-12135 |
| CVE | CVE-2020-15570 |
| XREF | USN:4450-1 |

Plugin Information

Published: 2020/08/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libwhoopsie0_0.2.69
- Fixed package : libwhoopsie0_0.2.69ubuntu0.1

- Installed package : whoopsie_0.2.69
- Fixed package : whoopsie_0.2.69ubuntu0.1

140267 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerabilities (USN-4488-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4488-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled the input extension protocol. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14346)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly initialized memory. A local attacker could possibly use this issue to obtain sensitive information. (CVE-2020-14347)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled the XkbSelectEvents function. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14361)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled the XRecordRegisterClients function. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14362)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4488-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-14346 |
| CVE | CVE-2020-14347 |
| CVE | CVE-2020-14361 |
| CVE | CVE-2020-14362 |
| XREF | USN:4488-1 |

Plugin Information

Published: 2020/09/04, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.8-2ubuntu2.3
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.8-2ubuntu2.3
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.8-2ubuntu2.3
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.3
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.8-2ubuntu2.3

143432 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerabilities (USN-4656-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4656-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server XKB extension incorrectly handled certain inputs. A local attacker could possibly use this issue to escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4656-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

CVE-2020-14360
CVE-2020-25712
XREF-USN:4656-1

Plugin Information

Published: 2020/12/02, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.8-2ubuntu2.6
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.8-2ubuntu2.6
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.8-2ubuntu2.6
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.6
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.8-2ubuntu2.6

140451 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4490-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4490-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled the XkbSetNames function. A local attacker could possibly use this issue to escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4490-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-14345 |
| XREF | USN:4490-1 |

Plugin Information

Published: 2020/09/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.8-2ubuntu2.4
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.8-2ubuntu2.4
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.8-2ubuntu2.4
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.4
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.8-2ubuntu2.4

[144011 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities \(USN-4665-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4665-1 advisory.

Marc Aldorasi discovered that curl incorrectly handled the libcurl CURLOPT_CONNECT_ONLY option. This could result in data being sent to the wrong destination, possibly exposing sensitive information. This issue only affected Ubuntu 20.10. (CVE-2020-8231)

Varnavas Papaioannou discovered that curl incorrectly handled FTP PASV responses. An attacker could possibly use this issue to trick curl into connecting to an arbitrary IP address and be used to perform port scanner and other information gathering. (CVE-2020-8284)

It was discovered that curl incorrectly handled FTP wildcard matchins. A remote attacker could possibly use this issue to cause curl to consume resources and crash, resulting in a denial of service.

(CVE-2020-8285)

It was discovered that curl incorrectly handled OCSP response verification. A remote attacker could possibly use this issue to provide a fraudulent OCSP response.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4665-1>

Solution

Update the affected 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

6.7 (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-2020-8231 |
| CVE | CVE-2020-8284 |
| CVE | CVE-2020-8285 |
| CVE | CVE-2020-8286 |
| XREF | USN:4665-1 |
| XREF | IAVA:2020-A-0581 |
| XREF | CEA-ID:CEA-2021-0025 |

Plugin Information

Published: 2020/12/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.4

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.4

148260 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-4898-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4898-1 advisory.

Viktor Szakats discovered that curl did not strip off user credentials from referrer header fields. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2021-22876)

Mingtao Yang discovered that curl incorrectly handled session tickets when using an HTTPS proxy. A remote attacker in control of an HTTPS proxy could use this issue to bypass certificate checks and intercept communications. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2021-22890)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4898-1>

Solution

Update the affected 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:L/I:N/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:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-22876 |
| CVE | CVE-2021-22890 |
| XREF | USN:4898-1 |

Plugin Information

Published: 2021/04/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.5

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.5

139724 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerability (USN-4466-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4466-1 advisory.

Marc Aldorasi discovered that curl incorrectly handled the libcurl CURLOPT_CONNECT_ONLY option. This could result in data being sent to the wrong destination, possibly exposing sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4466-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|--------------------|
| CVE | CVE-2020-8231 |
| XREF | USN:4466-1 |
| XREF | IAVA:2020-A-0389-S |

Plugin Information

Published: 2020/08/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.2
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.2

148089 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ldb vulnerabilities (USN-4888-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4888-1 advisory.

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain LDAP attributes. A remote attacker could possibly use this issue to cause the LDAP server to crash, resulting in a denial of service. (CVE-2021-20277)

Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain DN strings. A remote attacker could use this issue to cause the LDAP server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-27840)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4888-1>

Solution

Update the affected 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

6.5 (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-2020-27840 |
| CVE | CVE-2021-20277 |
| XREF | USN:4888-1 |
| XREF | IAVA:2021-A-0140-S |

Plugin Information

Published: 2021/03/24, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : liblldb2_2:2.0.10-0ubuntu0.20.04.1
- Fixed package : liblldb2_2:2.0.10-0ubuntu0.20.04.3
- Installed package : python3-lldb_2:2.0.10-0ubuntu0.20.04.1
- Fixed package : python3-lldb_2:2.0.10-0ubuntu0.20.04.3

148856 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libcaca vulnerability (USN-4921-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4921-1 advisory.

It was discovered that libcaca incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4921-1>

Solution

Update the affected caca-utils, libcaca-dev and / or libcaca0 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

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

CVSS v2.0 Temporal Score

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

References

CVE-2021-3410
XREF USN:4921-1

Plugin Information

Published: 2021/04/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcaca0_0.99.beta19-2.1ubuntu1
- Fixed package : libcaca0_0.99.beta19-2.1ubuntu1.20.04.1

237111 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libfcgi-perl vulnerability (USN-7527-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7527-1 advisory.

It was discovered that libfcgi-perl incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7527-1>

Solution

Update the affected libfcgi-perl package.

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)

References

CVE
XREF

CVE-2025-40907
USN:7527-1

Plugin Information

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

Plugin Output

tcp/0

- Installed package : libfcgi-perl_0.79-1
- Fixed package : libfcgi-perl_0.79-1ubuntu0.1

140643 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libproxy vulnerability (USN-4514-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4514-1 advisory.

It was discovered that libproxy incorrectly handled certain PAC files. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4514-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

CVE-2020-25219
XREF USN:4514-1

Plugin Information

Published: 2020/09/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libproxy1-plugin-gsettings_0.4.15-10ubuntu1
- Fixed package : libproxy1-plugin-gsettings_0.4.15-10ubuntu1.1
- Installed package : libproxy1-plugin-networkmanager_0.4.15-10ubuntu1
- Fixed package : libproxy1-plugin-networkmanager_0.4.15-10ubuntu1.1
- Installed package : libproxy1v5_0.4.15-10ubuntu1
- Fixed package : libproxy1v5_0.4.15-10ubuntu1.1

144704 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libproxy vulnerability (USN-4673-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4673-1 advisory.

Li Fei discovered that libproxy incorrectly handled certain PAC files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4673-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2020-26154](#)
XREF USN:4673-1

Plugin Information

Published: 2021/01/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libproxy1-plugin-gsettings_0.4.15-10ubuntu1
- Fixed package : libproxy1-plugin-gsettings_0.4.15-10ubuntu1.2
- Installed package : libproxy1-plugin-networkmanager_0.4.15-10ubuntu1
- Fixed package : libproxy1-plugin-networkmanager_0.4.15-10ubuntu1.2
- Installed package : libproxy1v5_0.4.15-10ubuntu1
- Fixed package : libproxy1v5_0.4.15-10ubuntu1.2

139367 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libssh vulnerability (USN-4447-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4447-1 advisory.

It was discovered that libssh incorrectly handled certain requests. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4447-1>

Solution

Update the affected 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:N/A:H)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-16135 |
| XREF | USN:4447-1 |

Plugin Information

Published: 2020/08/06, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libssh-4_0.9.3-2ubuntu2
- Fixed package : libssh-4_0.9.3-2ubuntu2.1

140266 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libx11 vulnerabilities (USN-4487-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4487-1 advisory.

Todd Carson discovered that libx11 incorrectly handled certain memory operations. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14344)

Jayden Rivers discovered that libx11 incorrectly handled locales. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14363)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4487-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2020-14344 |
| CVE | CVE-2020-14363 |
| XREF | USN:4487-1 |
| XREF | IAVB:2020-B-0051 |

Plugin Information

Published: 2020/09/04, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libx11-6_2:1.6.9-2ubuntu1
- Fixed package : libx11-6_2:1.6.9-2ubuntu1.1

- Installed package : libx11-data_2:1.6.9-2ubuntu1
- Fixed package : libx11-data_2:1.6.9-2ubuntu1.1

- Installed package : libx11-xcb1_2:1.6.9-2ubuntu1
- Fixed package : libx11-xcb1_2:1.6.9-2ubuntu1.1
```

144747 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : p11-kit vulnerabilities (USN-4677-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4677-1 advisory.

David Cook discovered that p11-kit incorrectly handled certain memory operations. An attacker could use this issue to cause p11-kit to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4677-1>

Solution

Update the affected 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:L/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-29361 |
| CVE | CVE-2020-29362 |
| CVE | CVE-2020-29363 |
| XREF | USN:4677-1 |

Plugin Information

Published: 2021/01/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libp11-kit0_0.23.20-1build1
- Fixed package : libp11-kit0_0.23.20-1ubuntu0.1
```

```
- Installed package : p11-kit_0.23.20-1build1
- Fixed package : p11-kit_0.23.20-1ubuntu0.1

- Installed package : p11-kit-modules_0.23.20-1build1
- Fixed package : p11-kit-modules_0.23.20-1ubuntu0.1
```

142368 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-cryptography vulnerability (USN-4613-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4613-1 advisory.

Hubert Kario discovered that python-cryptography incorrectly handled certain decryption. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4613-1>

Solution

Update the affected python-cryptography and / or python3-cryptography packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:H/V:I:H/V:A: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-25659 |
| XREF | USN:4613-1 |

Plugin Information

Published: 2020/11/04, Modified: 2024/09/19

Plugin Output

tcp/0

```
- Installed package : python3-cryptography_2.8-3
- Fixed package : python3-cryptography_2.8-3ubuntu0.1
```

146351 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : snapd vulnerability (USN-4728-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4728-1 advisory.

Gilad Reti and Nimrod Stoler discovered that snapd did not correctly specify cgroup delegation when generating systemd service units for various container management snaps. This could allow a local attacker to escalate privileges via access to arbitrary devices of the container host from within a compromised or malicious container.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4728-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-27352 |
| XREF | USN:4728-1 |

Plugin Information

Published: 2021/02/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.48.3+20.04

144944 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : tar vulnerabilities (USN-4692-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4692-1 advisory.

Chris Siebenmann discovered that tar incorrectly handled extracting files resized during extraction when invoked with the --sparse flag. An attacker could possibly use this issue to cause a denial of service.

This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

(CVE-2018-20482)

Daniel Axtens discovered that tar incorrectly handled certain malformed tar files. If a user or automated system were tricked into processing a specially crafted tar archive, a remote attacker could use this issue to cause tar to crash, resulting in a denial of service. (CVE-2019-9923)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4692-1>

Solution

Update the affected tar and / or tar-scripts 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

6.7 (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:N/A:P)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| BID | 106354 |
| CVE | CVE-2018-20482 |
| CVE | CVE-2019-9923 |
| XREF | USN:4692-1 |

Plugin Information

Published: 2021/01/14, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : tar_1.30+dfsg-7
- Fixed package : tar_1.30+dfsg-7ubuntu0.20.04.1

141177 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : urllib3 vulnerability (USN-4570-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4570-1 advisory.

It was discovered that urllib3 incorrectly handled certain character sequences. A remote attacker could possibly use this issue to perform CRLF injection.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4570-1>

Solution

Update the affected python-urllib3 and / or python3-urllib3 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:L/I:L/A:N)

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:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:O/RC:C)

References

CVE
XREF
CVE-2020-26137
USN:4570-1

Plugin Information

Published: 2020/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.25.8-2
- Fixed package : python3-urllib3_1.25.8-2ubuntu0.1

147984 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4757-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4757-1 advisory.

It was discovered that wpa_supplicant did not properly handle P2P (Wi-Fi Direct) provision discovery requests in some situations. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4757-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-27803 |
| XREF | USN:4757-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : wpasupplicant_2:2.9-1ubuntu4.1
- Fixed package : wpasupplicant_2:2.9-1ubuntu4.3

143268 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils vulnerability (USN-4649-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4649-1 advisory.

Jens Mueller discovered that xdg-utils incorrectly handled certain URI. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4649-1>

Solution

Update the affected xdg-utils package.

Risk Factor

Medium

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

4.3 (CVSS:2#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)

References

| | |
|------|----------------|
| CVE | CVE-2020-27748 |
| XREF | USN:4649-1 |

Plugin Information

Published: 2020/11/26, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : xdg-utils_1.1.3-2ubuntu1
- Fixed package : xdg-utils_1.1.3-2ubuntu1.20.04.1

178653 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory.

Hangyu Hua discovered that the Flower classifier implementation in the Linux kernel contained an out-of-bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-35788, LP: #2023577)

It was discovered that for some Intel processors the INVLPG instruction implementation did not properly flush global TLB entries when PCIDs are enabled. An attacker could use this to expose sensitive information (kernel memory) or possibly cause undesired behaviors. (LP: #2023220)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6193-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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-2023-35788 |
| XREF | USN:6193-1 |

Plugin Information

Published: 2023/07/20, Modified: 2024/09/19

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-153-generic for this advisory.

178914 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory.

It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3090)

Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges. (CVE-2023-32629)

It was discovered that the netfilter subsystem in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3390)

Tanguy Dubroca discovered that the netfilter subsystem in the Linux kernel did not properly handle certain pointer data type, leading to an out-of- bounds write vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35001)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6251-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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-2023-3090 |
| CVE | CVE-2023-3390 |
| CVE | CVE-2023-32629 |
| CVE | CVE-2023-35001 |
| XREF | USN:6251-1 |

Plugin Information

Published: 2023/07/26, Modified: 2025/03/31

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-155-generic for this advisory.

179704 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6284-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6284-1 advisory.

It was discovered that the netlink implementation in the Linux kernel did not properly validate policies when parsing attributes in some situations. An attacker could use this to cause a denial of service (infinite recursion). (CVE-2020-36691)

Billy Jheng Bing Jhong discovered that the CIFS network file system implementation in the Linux kernel did not properly validate arguments to ioctl() in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-0168)

It was discovered that the ext4 file system implementation in the Linux kernel contained a use-after-free vulnerability. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2022-1184)

It was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using a return address from a sibling thread. A local attacker could possibly use this to expose sensitive information. (CVE-2022-27672)

William Zhao discovered that the Traffic Control (TC) subsystem in the Linux kernel did not properly handle network packet retransmission in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-4269)

It was discovered that a race condition existed in the qdisc implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0590)

It was discovered that a race condition existed in the btrfs file system implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1611)

It was discovered that the APM X-Gene SoC hardware monitoring driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-1855)

It was discovered that the ST NCI NFC driver did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2023-1990)

It was discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation when mounting certain images. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service (system crash). (CVE-2023-2124)

It was discovered that the SLIMpro I2C device driver in the Linux kernel did not properly validate user-supplied data in some situations, leading to an out-of-bounds write vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-2194)

It was discovered that a race condition existed in the TLS subsystem in the Linux kernel, leading to a use-after-free or a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-28466)

It was discovered that the DA9150 charger driver in the Linux kernel did not properly handle device removal, leading to a user-after free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-30772)

It was discovered that the btrfs file system implementation in the Linux kernel did not properly handle error conditions in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-3111)

It was discovered that the Ricoh R5C592 MemoryStick card reader driver in the Linux kernel contained a race condition during module unload, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3141)

It was discovered that the Qualcomm EMAC ethernet driver in the Linux kernel did not properly handle device removal, leading to a user-after free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-33203)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6284-1>

Solution

Update the affected kernel package.

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-2020-36691
CVE CVE-2022-0168
CVE CVE-2022-1184
CVE CVE-2022-4269
CVE CVE-2022-27672
CVE CVE-2023-0590
CVE CVE-2023-1611
CVE CVE-2023-1855
CVE CVE-2023-1990
CVE CVE-2023-2124
CVE CVE-2023-2194
CVE CVE-2023-3111
CVE CVE-2023-3141
CVE CVE-2023-28466
CVE CVE-2023-30772
CVE CVE-2023-33203
XREF USN:6284-1

Plugin Information

Published: 2023/08/11, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-156-generic for this advisory.

180257 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6317-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6317-1 advisory.

Daniel Moghimi discovered that some Intel(R) Processors did not properly clear microarchitectural state after speculative execution of various instructions. A local unprivileged user could use this to obtain sensitive information. (CVE-2022-40982)

Tavis Ormandy discovered that some AMD processors did not properly handle speculative execution of certain vector register instructions. A local attacker could use this to expose sensitive information.
(CVE-2023-20593)

It was discovered that the universal 32bit network packet classifier implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3609)

It was discovered that the Quick Fair Queueing network scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3611)

It was discovered that the network packet classifier with netfilter/firewall marks implementation in the Linux kernel did not properly handle reference counting, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3776)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6317-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

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-2022-40982 |
| CVE | CVE-2023-3609 |
| CVE | CVE-2023-3611 |
| CVE | CVE-2023-3776 |
| CVE | CVE-2023-20593 |
| XREF | USN:6317-1 |

Plugin Information

Published: 2023/08/29, Modified: 2024/09/19

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-159-generic for this advisory.

180512 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6340-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6340-1 advisory.

Ruihan Li discovered that the bluetooth subsystem in the Linux kernel did not properly perform permissions checks when handling HCI sockets. A physically proximate attacker could use this to cause a denial of service (bluetooth communication). (CVE-2023-2002)

Zi Fan Tan discovered that the binder IPC implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-21255)

Juan Jose Lopez Jaimez, Meador Inge, Simon Scannell, and Nenad Stojanovski discovered that the BPF verifier in the Linux kernel did not properly mark registers for precision tracking in certain situations, leading to an out- of-bounds access vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-2163)

Zheng Zhang discovered that the device-mapper implementation in the Linux kernel did not properly handle locking during table_clear() operations. A local

attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2269)

It was discovered that the DVB Core driver in the Linux kernel did not properly handle locking events in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock).

(CVE-2023-31084)

It was discovered that the kernel->user space relay implementation in the Linux kernel did not properly perform certain buffer calculations, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-3268)

It was discovered that the video4linux driver for Philips based TV cards in the Linux kernel contained a race condition during device removal, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35823)

It was discovered that the SDMC DM1105 PCI device driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35824)

It was discovered that the Renesas USB controller driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35828)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6340-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C: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: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-2023-2002 |
| CVE | CVE-2023-2163 |
| CVE | CVE-2023-2269 |
| CVE | CVE-2023-3268 |
| CVE | CVE-2023-21255 |
| CVE | CVE-2023-31084 |
| CVE | CVE-2023-35823 |
| CVE | CVE-2023-35824 |
| CVE | CVE-2023-35828 |
| XREF | USN:6340-1 |

Plugin Information

Published: 2023/09/05, Modified: 2024/09/18

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-163-generic for this advisory.

181641 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6387-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6387-1 advisory.

Jana Hofmann, Emanuele Vannacci, Cedric Fournet, Boris Kopf, and Oleksii Oleksenko discovered that some AMD processors could leak stale data from division operations in certain situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-20588)

It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle L2CAP socket release, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-40283)

It was discovered that some network classifier implementations in the Linux kernel contained use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4128)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6387-1>

Solution

Update the affected kernel package.

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 (CVSS:2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS:2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2023-4128 |
| CVE | CVE-2023-20588 |
| CVE | CVE-2023-40283 |
| XREF | USN:6387-1 |

Plugin Information

Published: 2023/09/19, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-163-generic for this advisory.

182578 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6417-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6417-1 advisory.

It was discovered that the eBPF implementation in the Linux kernel contained a race condition around read-only maps. A privileged attacker could use this to modify read-only maps. (CVE-2021-4001)

It was discovered that the IPv6 implementation in the Linux kernel contained a high rate of hash collisions in connection lookup table. A remote attacker could use this to cause a denial of service (excessive CPU consumption). (CVE-2023-1206)

Yang Lan discovered that the GFS2 file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious GFS2 image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2023-3212)

Davide Ornaghi discovered that the DECnet network protocol implementation in the Linux kernel contained a null pointer dereference vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. Please note that kernel support for the DECnet has been removed to resolve this CVE. (CVE-2023-3338)

It was discovered that the NFC implementation in the Linux kernel contained a use-after-free vulnerability when performing peer-to-peer communication in certain conditions. A privileged attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2023-3863)

It was discovered that the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-4194)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6417-1>

Solution

Update the affected kernel package.

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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2021-4001 |
| CVE | CVE-2023-1206 |
| CVE | CVE-2023-3212 |
| CVE | CVE-2023-3338 |
| CVE | CVE-2023-3863 |
| CVE | CVE-2023-4194 |
| XREF | USN:6417-1 |

Plugin Information

Published: 2023/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates

require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-164-generic for this advisory.

183455 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6441-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6441-1 advisory.

Ross Lagerwall discovered that the Xen netback backend driver in the Linux kernel did not properly handle certain unusual packets from a paravirtualized network frontend, leading to a buffer overflow. An attacker in a guest VM could use this to cause a denial of service (host system crash) or possibly execute arbitrary code. (CVE-2023-34319)

Kyle Zeng discovered that the networking stack implementation in the Linux kernel did not properly validate skb object size in certain conditions. An attacker could use this cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42752)

Kyle Zeng discovered that the netfiler subsystem in the Linux kernel did not properly calculate array offsets, leading to a out-of-bounds write vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42753)

Kyle Zeng discovered that the IPv4 Resource Reservation Protocol (RSVP) classifier implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash). Please note that kernel packet classifier support for RSVP has been removed to resolve this vulnerability. (CVE-2023-42755)

Kyle Zeng discovered that the netfilter subsystem in the Linux kernel contained a race condition in IP set operations in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-42756)

Bing-Jhong Billy Jheng discovered that the Unix domain socket implementation in the Linux kernel contained a race condition in certain situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4622)

Budimir Markovic discovered that the qdisc implementation in the Linux kernel did not properly validate inner classes, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4623)

Alex Birnberg discovered that the netfilter subsystem in the Linux kernel did not properly validate register length, leading to an out-of- bounds write vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-4881)

It was discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel did not properly handle network packets in certain conditions, leading to a use after free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4921)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6441-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-4622 |
| CVE | CVE-2023-4623 |
| CVE | CVE-2023-4881 |
| CVE | CVE-2023-4921 |
| CVE | CVE-2023-34319 |
| CVE | CVE-2023-42752 |
| CVE | CVE-2023-42753 |
| CVE | CVE-2023-42755 |
| CVE | CVE-2023-42756 |
| XREF | USN:6441-1 |

Plugin Information

Published: 2023/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-165-generic for this advisory.

184085 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6462-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6462-1 advisory.

Seth Jenkins discovered that the Linux kernel did not properly perform address randomization for a per-cpu memory management structure. A local attacker could use this to expose sensitive information (kernel memory) or in conjunction with another kernel vulnerability. (CVE-2023-0597)

Yu Hao and Weiteng Chen discovered that the Bluetooth HCI UART driver in the Linux kernel contained a race condition, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-31083)

Lin Ma discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a null pointer dereference vulnerability in some situations. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-3772)

It was discovered that the Siano USB MDTV receiver device driver in the Linux kernel did not properly handle device initialization failures in certain situations, leading to a use-after-free vulnerability. A physically proximate attacker could use this cause a denial of service (system crash). (CVE-2023-4132)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6462-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-0597 |
| CVE | CVE-2023-3772 |
| CVE | CVE-2023-4132 |
| CVE | CVE-2023-31083 |
| XREF | USN:6462-1 |

Plugin Information

Published: 2023/10/31, Modified: 2024/08/28

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-166-generic for this advisory.

186082 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6495-1 advisory.

Yu Hao discovered that the UBI driver in the Linux kernel did not properly check for MTD with zero erasesize during device attachment. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-31085)

Manfred Rudiger discovered that the Intel(R) PCI-Express Gigabit (igb) Ethernet driver in the Linux kernel did not properly validate received frames that are larger than the set MTU size, leading to a buffer overflow vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-45871)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6495-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-31085 |
| CVE | CVE-2023-45871 |
| XREF | USN:6495-1 |

Plugin Information

Published: 2023/11/21, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-167-generic for this advisory.

189614 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6605-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6605-1 advisory.

Lin Ma discovered that the netfilter subsystem in the Linux kernel did not properly validate network family support while creating a new netfilter table. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6040)

It was discovered that the CIFS network file system implementation in the Linux kernel did not properly validate the server frame size in certain situation, leading to an out-of-bounds read vulnerability. An attacker could use this to construct a malicious CIFS image that, when operated on, could cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-6606)

Budimir Markovic, Lucas De Marchi, and Pengfei Xu discovered that the perf subsystem in the Linux kernel did not properly validate all event sizes when attaching new events, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6931)

It was discovered that the IGMP protocol implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6932)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6605-1>

Solution

Update the affected kernel package.

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-2023-6040 |
| CVE | CVE-2023-6606 |
| CVE | CVE-2023-6931 |
| CVE | CVE-2023-6932 |
| XREF | USN:6605-1 |

Plugin Information

Published: 2024/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-170-generic for this advisory.

190124 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6625-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6625-1 advisory.

Marek Marczykowski-Grecki discovered that the Xen event channel infrastructure implementation in the Linux kernel contained a race condition. An attacker in a guest VM could possibly use this to cause a denial of service (paravirtualized device unavailability). (CVE-2023-34324)

Zheng Wang discovered a use-after-free in the Renesas Ethernet AVB driver in the Linux kernel during device removal. A privileged attacker could use this to cause a denial of service (system crash).

(CVE-2023-35827)

It was discovered that a race condition existed in the Linux kernel when performing operations with kernel objects, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2023-45863)

discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel did not properly handle certain memory allocation failure conditions, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2023-46343)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6625-1>

Solution

Update the affected kernel package.

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

6.1 (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)

References

| | |
|------|----------------|
| CVE | CVE-2023-34324 |
| CVE | CVE-2023-35827 |
| CVE | CVE-2023-45863 |
| CVE | CVE-2023-46343 |
| XREF | USN:6625-1 |

Plugin Information

Published: 2024/02/08, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-171-generic for this advisory.

176550 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6128-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6128-1 advisory.

It was discovered that CUPS incorrectly handled logging. A remote attacker could use this issue to cause CUPS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6128-1>

Solution

Update the affected 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-2023-32324 |
| XREF | USN:6128-1 |

Plugin Information

Published: 2023/06/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.3
- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.3
- Installed package : cups-client_2.3.1-9ubuntu1.1

- Fixed package : cups-client_2.3.1-9ubuntu1.3
- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.3
- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.3
- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.3
- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.3
- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.3
- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.3
- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.3
- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.3

201188 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : eSpeak NG vulnerabilities (USN-6858-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6858-1 advisory.

It was discovered that eSpeak NG did not properly manage memory under certain circumstances. An attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2023-49990, CVE-2023-49991, CVE-2023-49992, CVE-2023-49993, CVE-2023-49994)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6858-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-49990 |
| CVE | CVE-2023-49991 |
| CVE | CVE-2023-49992 |
| CVE | CVE-2023-49993 |
| CVE | CVE-2023-49994 |
| XREF | USN:6858-1 |

Plugin Information

Published: 2024/07/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : espeak-ng-data_1.50+dfsg-6
- Fixed package : espeak-ng-data_1.50+dfsg-6ubuntu0.1
- Installed package : libespeak-ng1_1.50+dfsg-6
- Fixed package : libespeak-ng1_1.50+dfsg-6ubuntu0.1

215062 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU C Library vulnerability (USN-7259-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7259-1 advisory.

It was discovered that GNU C Library incorrectly handled memory when using the assert function. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7259-1>

Solution

Update the affected 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

6.5 (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-2025-0395 |
| XREF | IAVA:2025-A-0062 |
| XREF | USN:7259-1 |

Plugin Information

Published: 2025/02/06, Modified: 2025/02/06

Plugin Output

tcp/0

- Installed package : libc-bin_2.31-0ubuntu9
- Fixed package : libc-bin_2.31-0ubuntu9.17

```
- Installed package : libc-dev-bin_2.31-0ubuntu9
- Fixed package : libc-dev-bin_2.31-0ubuntu9.17

- Installed package : libc6_2.31-0ubuntu9
- Fixed package : libc6_2.31-0ubuntu9.17

- Installed package : locales_2.31-0ubuntu9
- Fixed package : locales_2.31-0ubuntu9.17
```

161252 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apport vulnerabilities (USN-5427-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5427-1 advisory.

Muqing Liu and neoni discovered that Apport incorrectly handled detecting if an executable was replaced after a crash. A local attacker could possibly use this issue to execute arbitrary code as the root user.

(CVE-2021-3899)

Gerrit Venema discovered that Apport incorrectly handled connections to Apport sockets inside containers.

A local attacker could possibly use this issue to connect to arbitrary sockets as the root user.

(CVE-2022-1242)

Gerrit Venema discovered that Apport incorrectly handled user settings files. A local attacker could possibly use this issue to cause Apport to consume resources, leading to a denial of service.

(CVE-2022-28652)

Gerrit Venema discovered that Apport did not limit the amount of logging from D-Bus connections. A local attacker could possibly use this issue to fill up the Apport log file, leading to denial of service.

(CVE-2022-28654)

Gerrit Venema discovered that Apport did not filter D-Bus connection strings. A local attacker could possibly use this issue to cause Apport to make arbitrary network connections. (CVE-2022-28655)

Gerrit Venema discovered that Apport did not limit the amount of memory being consumed during D-Bus connections. A local attacker could possibly use this issue to cause Apport to consume memory, leading to a denial of service. (CVE-2022-28656)

Gerrit Venema discovered that Apport did not disable the python crash handler before chrooting into a container. A local attacker could possibly use this issue to execute arbitrary code. (CVE-2022-28657)

Gerrit Venema discovered that Apport incorrectly handled filename argument whitespace. A local attacker could possibly use this issue to spoof arguments to the Apport daemon. (CVE-2022-28658)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5427-1>

Solution

Update the affected 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-2021-3899 |
| CVE | CVE-2022-1242 |
| CVE | CVE-2022-28652 |
| CVE | CVE-2022-28654 |
| CVE | CVE-2022-28655 |
| CVE | CVE-2022-28656 |
| CVE | CVE-2022-28657 |
| CVE | CVE-2022-28658 |
| XREF | USN:5427-1 |

Plugin Information

Published: 2022/05/17, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.24
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.24
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.24
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.24

174274 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apport vulnerability (USN-6018-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6018-1 advisory.

Chen Lu, Lei Wang, and YiQi Sun discovered a privilege escalation vulnerability in apport-cli when viewing crash reports and unprivileged users are allowed to run sudo less. A local attacker on a specially configured system could use this to escalate their privilege.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6018-1>

Solution

Update the affected 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-2023-1326 |
| XREF | USN:6018-1 |

Plugin Information

Published: 2023/04/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.26
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.26
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.26
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.26

165706 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : DHCP vulnerabilities (USN-5658-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5658-1 advisory.

It was discovered that DHCP incorrectly handled option reference counting. A remote attacker could possibly use this issue to cause DHCP servers to crash, resulting in a denial of service. (CVE-2022-2928)

It was discovered that DHCP incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause DHCP clients and servers to consume resources, leading to a denial of service. (CVE-2022-2929)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5658-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2022-2928 |
| CVE | CVE-2022-2929 |
| XREF | USN:5658-1 |
| XREF | IAVB:2022-B-0037 |

Plugin Information

Published: 2022/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : isc-dhcp-client_4.4.1-2.1ubuntu5
- Fixed package : isc-dhcp-client_4.4.1-2.1ubuntu5.20.04.4
- Installed package : isc-dhcp-common_4.4.1-2.1ubuntu5
- Fixed package : isc-dhcp-common_4.4.1-2.1ubuntu5.20.04.4

161908 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeRDP vulnerabilities (USN-5461-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5461-1 advisory.

It was discovered that FreeRDP incorrectly handled empty password values. A remote attacker could use this issue to bypass server authentication. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-24882)

It was discovered that FreeRDP incorrectly handled server configurations with an invalid SAM file path. A remote attacker could use this issue to bypass server authentication. (CVE-2022-24883)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5461-1>

Solution

Update the affected 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)

References

| | |
|------|----------------|
| CVE | CVE-2022-24882 |
| CVE | CVE-2022-24883 |
| XREF | USN:5461-1 |

Plugin Information

Published: 2022/06/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.3
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.3
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.3

169587 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNOME Files vulnerability (USN-5786-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5786-1 advisory.

It was discovered that GNOME Files incorrectly handled certain filenames. An attacker could possibly use this issue to cause GNOME Files to crash, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5786-1>

Solution

Update the affected 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-2022-37290 |
| XREF | USN:5786-1 |

Plugin Information

Published: 2023/01/05, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnautilus-extension1a_1:3.36.3-0ubuntu1
- Fixed package : libnautilus-extension1a_1:3.36.3-0ubuntu1.20.04.2

- Installed package : nautilus_1:3.36.3-0ubuntu1
- Fixed package : nautilus_1:3.36.3-0ubuntu1.20.04.2
- Installed package : nautilus-data_1:3.36.3-0ubuntu1
- Fixed package : nautilus-data_1:3.36.3-0ubuntu1.20.04.2

165504 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerabilities (USN-5643-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5643-1 advisory.

It was discovered that GhostScript incorrectly handled certain PDF files. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to cause GhostScript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-27792)

It was discovered that GhostScript incorrectly handled certain PDF files. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to cause GhostScript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2085)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5643-1>

Solution

Update the affected 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:N/I:H/A:H)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2020-27792 |
| CVE | CVE-2022-2085 |
| XREF | USN:5643-1 |
| XREF | IAVB:2022-B-0034-S |

Plugin Information

Published: 2022/09/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.6

```
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.6

- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.6

- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.6
```

162734 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuPG vulnerability (USN-5503-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5503-1 advisory.

Demi Marie Obenour discovered that GnuPG incorrectly handled injection in the status message. A remote attacker could possibly use this issue to forge signatures.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5503-1>

Solution

Update the affected packages.

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](#)
XREF USN:5503-1

Plugin Information

Published: 2022/07/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : dirmngr_2.2.19-3ubuntu2
- Fixed package : dirmngr_2.2.19-3ubuntu2.2

- Installed package : gnupg_2.2.19-3ubuntu2
- Fixed package : gnupg_2.2.19-3ubuntu2.2

- Installed package : gnupg-l10n_2.2.19-3ubuntu2
- Fixed package : gnupg-l10n_2.2.19-3ubuntu2.2

- Installed package : gnupg-utils_2.2.19-3ubuntu2
- Fixed package : gnupg-utils_2.2.19-3ubuntu2.2

- Installed package : gpg_2.2.19-3ubuntu2
- Fixed package : gpg_2.2.19-3ubuntu2.2
```

```
- Installed package : gpg-agent_2.2.19-3ubuntu2
- Fixed package : gpg-agent_2.2.19-3ubuntu2.2

- Installed package : gpg-wks-client_2.2.19-3ubuntu2
- Fixed package : gpg-wks-client_2.2.19-3ubuntu2.2

- Installed package : gpg-wks-server_2.2.19-3ubuntu2
- Fixed package : gpg-wks-server_2.2.19-3ubuntu2.2

- Installed package : gpgconf_2.2.19-3ubuntu2
- Fixed package : gpgconf_2.2.19-3ubuntu2.2

- Installed package : gpgsm_2.2.19-3ubuntu2
- Fixed package : gpgsm_2.2.19-3ubuntu2.2

- Installed package : gpgv_2.2.19-3ubuntu2
- Fixed package : gpgv_2.2.19-3ubuntu2.2
```

163106 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : HTTP-Daemon vulnerability (USN-5520-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5520-1 advisory.

It was discovered that HTTP-Daemon incorrectly handled certain crafted requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5520-1>

Solution

Update the affected libhttp-daemon-perl package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS 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)

References

| | |
|------|----------------|
| CVE | CVE-2022-31081 |
| XREF | USN:5520-1 |

Plugin Information

Published: 2022/07/14, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libhttp-daemon-perl_6.06-1
- Fixed package : libhttp-daemon-perl_6.06-1ubuntu0.1
```

162404 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerabilities (USN-5486-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5486-1 advisory.

It was discovered that some Intel processors did not implement sufficient control flow management. A local attacker could use this to cause a denial of service. (CVE-2021-0127)

Joseph Nuzman discovered that some Intel processors did not properly initialise shared resources. A local attacker could use this to obtain sensitive information. (CVE-2021-0145)

Mark Ermolov, Dmitry Sklyarov and Maxim Goryachy discovered that some Intel processors did not prevent test and debug logic from being activated at runtime. A local attacker could use this to escalate privileges. (CVE-2021-0146)

It was discovered that some Intel processors did not properly restrict access in some situations. A local attacker could use this to obtain sensitive information. (CVE-2021-33117)

Brandon Miller discovered that some Intel processors did not properly restrict access in some situations.

A local attacker could use this to obtain sensitive information or a remote attacker could use this to cause a denial of service. (CVE-2021-33120)

It was discovered that some Intel processors did not completely perform cleanup actions on multi-core shared buffers. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21123, CVE-2022-21127)

Alysa Milburn, Jason Brandt, Avishai Redelman and Nir Lavi discovered that some Intel processors improperly optimised security-critical code. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21151)

It was discovered that some Intel processors did not properly perform cleanup during specific special register write operations. A local attacker could possibly use this to expose sensitive information.

(CVE-2022-21166)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5486-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2021-0127 |
| CVE | CVE-2021-0145 |
| CVE | CVE-2021-0146 |
| CVE | CVE-2021-33117 |
| CVE | CVE-2021-33120 |
| CVE | CVE-2022-21123 |
| CVE | CVE-2022-21127 |
| CVE | CVE-2022-21151 |
| CVE | CVE-2022-21166 |

XREF

USN:5486-1

Plugin Information

Published: 2022/06/20, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20220510.0ubuntu0.20.04.1

165109 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerability (USN-5612-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5612-1 advisory.

Pietro Borrello, Andreas Kogler, Martin Schwarzl, Daniel Gruss, Michael Schwarz and Moritz Lipp discovered that some Intel processors did not properly clear data between subsequent xAPIC MMIO reads. This could allow a local attacker to compromise SGX enclaves.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5612-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE
XREF

CVE-2022-21233
USN:5612-1

Plugin Information

Published: 2022/09/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20220809.0ubuntu0.20.04.1

162172 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5476-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5476-1 advisory.

Han Zheng discovered that Liblouis incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. This issue was addressed in Ubuntu 21.10 and Ubuntu 22.04 LTS. (CVE-2022-26981)

It was discovered that Liblouis incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2022-31783)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5476-1>

Solution

Update the affected 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-2022-26981 |
| CVE | CVE-2022-31783 |
| XREF | USN:5476-1 |

Plugin Information

Published: 2022/06/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : liblouis-data_3.12.0-3
- Fixed package : liblouis-data_3.12.0-3ubuntu0.1
- Installed package : liblouis20_3.12.0-3
- Fixed package : liblouis20_3.12.0-3ubuntu0.1
- Installed package : python3-louis_3.12.0-3
- Fixed package : python3-louis_3.12.0-3ubuntu0.1

166339 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibreOffice vulnerabilities (USN-5694-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5694-1 advisory.

It was discovered that LibreOffice incorrectly handled links using the Office URI Schemes. If a user were tricked into opening a specially crafted document, a remote attacker could use this issue to execute arbitrary scripts. (CVE-2022-3140)

Thomas Florian discovered that LibreOffice incorrectly handled crashes when an encrypted document is open.

If the document is recovered upon restarting LibreOffice, subsequent saves of the document were unencrypted. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-12801)

Jens Mller discovered that LibreOffice incorrectly handled certain documents containing forms. If a user were tricked into opening a specially crafted document, a remote attacker could overwrite arbitrary files when the form was submitted. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-12803)

It was discovered that LibreOffice incorrectly validated macro signatures. If a user were tricked into opening a specially crafted document, a remote attacker could possibly use this issue to execute arbitrary macros. This issue only affected Ubuntu 18.04 LTS. (CVE-2022-26305)

It was discovered that LibreOffice incorrectly handled encrypting the master key provided by the user for storing passwords for web connections. A local attacker could possibly use this issue to obtain access to passwords stored in the users configuration data. This issue only affected Ubuntu 18.04 LTS. (CVE-2022-26306, CVE-2022-26307)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5694-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C: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-2020-12801 |
| CVE | CVE-2020-12803 |
| CVE | CVE-2022-3140 |
| CVE | CVE-2022-26305 |
| CVE | CVE-2022-26306 |
| CVE | CVE-2022-26307 |
| XREF | USN:5694-1 |
| XREF | IAVB:2022-B-0024-S |
| XREF | IAVB:2022-B-0040-S |

Plugin Information

Published: 2022/10/20, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1

- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.6
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libuno-purpenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.6
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.6
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1

- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.6
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.6
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.6

164327 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libxslt vulnerabilities (USN-5575-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5575-1 advisory.

Nicolas Grgoire discovered that Libxslt incorrectly handled certain XML. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-5815)

Alexey Neyman incorrectly handled certain HTML pages. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code. (CVE-2021-30560)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5575-1>

Solution

Update the affected 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 |
| XREF | USN:5575-1 |

Plugin Information

Published: 2022/08/22, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libxslt1.1_1.1.34-4
- Fixed package : libxslt1.1_1.1.34-4ubuntu0.20.04.1

160474 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5400-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5400-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.29 in Ubuntu 20.04 LTS, Ubuntu 21.10, and Ubuntu 22.04 LTS. Ubuntu 18.04 LTS has been updated to MySQL 5.7.38.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-38.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-29.html>
<https://www.oracle.com/security-alerts/cpuapr2022.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5400-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|-----|----------------|
| CVE | CVE-2022-21412 |
| CVE | CVE-2022-21413 |
| CVE | CVE-2022-21414 |
| CVE | CVE-2022-21415 |
| CVE | CVE-2022-21417 |
| CVE | CVE-2022-21418 |
| CVE | CVE-2022-21423 |
| CVE | CVE-2022-21425 |
| CVE | CVE-2022-21427 |
| CVE | CVE-2022-21435 |
| CVE | CVE-2022-21436 |
| CVE | CVE-2022-21437 |
| CVE | CVE-2022-21438 |
| CVE | CVE-2022-21440 |
| CVE | CVE-2022-21444 |
| CVE | CVE-2022-21451 |
| CVE | CVE-2022-21452 |
| CVE | CVE-2022-21454 |
| CVE | CVE-2022-21457 |
| CVE | CVE-2022-21459 |
| CVE | CVE-2022-21460 |
| CVE | CVE-2022-21462 |
| CVE | CVE-2022-21478 |

XREF USN:5400-1
XREF IAVA:2022-A-0168-S

Plugin Information

Published: 2022/05/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.29-0ubuntu0.20.04.2

163522 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5537-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5537-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.30 in Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. Ubuntu 18.04 LTS has been updated to MySQL 5.7.39.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-39.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-30.html>
<https://www.oracle.com/security-alerts/cpujul2022.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5537-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|-----|--------------------------------|
| CVE | CVE-2022-21509 |
| CVE | CVE-2022-21515 |
| CVE | CVE-2022-21517 |
| CVE | CVE-2022-21522 |
| CVE | CVE-2022-21525 |
| CVE | CVE-2022-21526 |
| CVE | CVE-2022-21527 |

| | |
|------|----------------|
| CVE | CVE-2022-21528 |
| CVE | CVE-2022-21529 |
| CVE | CVE-2022-21530 |
| CVE | CVE-2022-21531 |
| CVE | CVE-2022-21534 |
| CVE | CVE-2022-21537 |
| CVE | CVE-2022-21538 |
| CVE | CVE-2022-21539 |
| CVE | CVE-2022-21547 |
| CVE | CVE-2022-21553 |
| CVE | CVE-2022-21569 |
| XREF | USN:5537-1 |

Plugin Information

Published: 2022/07/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.30-0ubuntu0.20.04.2
```

166452 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5696-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5696-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.31 in Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. Ubuntu 18.04 LTS has been updated to MySQL 5.7.40.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-40.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-31.html>
<https://www.oracle.com/security-alerts/cpuoct2022.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5696-1>

Solution

Update the affected 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)

References

| | |
|------|----------------|
| CVE | CVE-2022-21589 |
| CVE | CVE-2022-21592 |
| CVE | CVE-2022-21594 |
| CVE | CVE-2022-21599 |
| CVE | CVE-2022-21604 |
| CVE | CVE-2022-21608 |
| CVE | CVE-2022-21611 |
| CVE | CVE-2022-21617 |
| CVE | CVE-2022-21625 |
| CVE | CVE-2022-21632 |
| CVE | CVE-2022-21633 |
| CVE | CVE-2022-21637 |
| CVE | CVE-2022-21640 |
| CVE | CVE-2022-39400 |
| CVE | CVE-2022-39408 |
| CVE | CVE-2022-39410 |
| XREF | USN:5696-1 |

Plugin Information

Published: 2022/10/25, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.31-0ubuntu0.20.04.1

166861 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NTFS-3G vulnerability (USN-5711-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5711-1 advisory.

Yuchen Zeng and Eduardo Vela discovered that NTFS-3G incorrectly validated certain NTFS metadata. A local attacker could possibly use this issue to gain privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5711-1>

Solution

Update the affected 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:I/C:A;C)

CVSS v2.0 Temporal Score

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

References

CVE-2022-40284
XREF USN:5711-1

Plugin Information

Published: 2022/11/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1
- Fixed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1.3
- Installed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1
- Fixed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1.3

164376 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Open VM Tools vulnerability (USN-5578-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5578-1 advisory.

It was discovered that Open VM Tools incorrectly handled certain requests. An attacker inside the guest could possibly use this issue to gain root privileges inside the virtual machine.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5578-1>

Solution

Update the affected 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-31676
XREF USN:5578-1
XREF IAVB:2022-B-0029-S

Plugin Information

Published: 2022/08/24, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : open-vm-tools_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools_2:11.3.0-2ubuntu0~ubuntu20.04.3

- Installed package : open-vm-tools-desktop_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools-desktop_2:11.3.0-2ubuntu0~ubuntu20.04.3

172495 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Protocol Buffers vulnerabilities (USN-5945-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5945-1 advisory.

It was discovered that Protocol Buffers did not properly validate field com.google.protobuf.UnknownFieldSet in protobuf-java. An attacker could possibly use this issue to perform a denial of service attack. This issue only affected protobuf Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2021-22569)

It was discovered that Protocol Buffers did not properly parse certain symbols. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. (CVE-2021-22570)

It was discovered that Protocol Buffers did not properly manage memory when parsing specifically crafted messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-1941)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5945-1>

Solution

Update the affected 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 (CVSS:2.0/AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS:2.0/POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-22569 |
| CVE | CVE-2021-22570 |
| CVE | CVE-2022-1941 |
| XREF | USN:5945-1 |

Plugin Information

Published: 2023/03/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libprotobuf17_3.6.1.3-2ubuntu5

- Fixed package : libprotobuf17_3.6.1.3-2ubuntu5.2
- Installed package : python3-protobuf_3.6.1.3-2ubuntu5
- Fixed package : python3-protobuf_3.6.1.3-2ubuntu5.2

163294 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : PyJWT vulnerability (USN-5526-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5526-1 advisory.

Aapo Oksman discovered that PyJWT incorrectly handled signatures constructed from SSH public keys. A remote attacker could use this to forge a JWT signature.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5526-1>

Solution

Update the affected python-jwt and / or python3-jwt 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-2022-29217 |
| XREF | USN:5526-1 |

Plugin Information

Published: 2022/07/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-jwt_1.7.1-2ubuntu2
- Fixed package : python3-jwt_1.7.1-2ubuntu2.1

160674 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Rsyslog vulnerability (USN-5404-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5404-1 advisory.

Pieter Agten discovered that Rsyslog incorrectly handled certain requests. An attacker could possibly use this issue to cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5404-1>

Solution

Update the affected packages.

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
XREF USN:5404-1

Plugin Information

Published: 2022/05/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : rsyslog_8.2001.0-1ubuntu1
- Fixed package : rsyslog_8.2001.0-1ubuntu1.3

170178 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Sudo vulnerabilities (USN-5811-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5811-1 advisory.

Matthieu Barjole and Victor Cutillas discovered that Sudo incorrectly handled user-specified editors when using the sudoedit command. A local attacker that has permission to use the sudoedit command could possibly use this issue to edit arbitrary files. (CVE-2023-22809)

It was discovered that the Protobuf-c library, used by Sudo, incorrectly handled certain arithmetic shifts. An attacker could possibly use this issue to cause Sudo to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-33070)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5811-1>

Solution

Update the affected sudo and / or sudo-ldap 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

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:H/RL:O/RC:C)

References

CVE CVE-2022-33070
CVE CVE-2023-22809
XREF USN:5811-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2023/01/19, Modified: 2024/09/11

Plugin Output

tcp/0

- Installed package : sudo_1.8.31-1ubuntu1
- Fixed package : sudo_1.8.31-1ubuntu1.4

174161 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Sudo vulnerabilities (USN-6005-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6005-1 advisory.

Matthieu Barjole and Victor Cutilas discovered that Sudo incorrectly escaped control characters in log messages and sudoreplay output. An attacker could possibly use these issues to inject terminal control characters that alter output when being viewed.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6005-1>

Solution

Update the affected sudo and / or sudo-ldap 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:L/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

| | |
|------|--------------------|
| CVE | CVE-2023-28486 |
| CVE | CVE-2023-28487 |
| XREF | USN:6005-1 |
| XREF | IAVA:2023-A-0121-S |

Plugin Information

Published: 2023/04/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : sudo_1.8.31-1ubuntu1
- Fixed package : sudo_1.8.31-1ubuntu1.5

165188 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5613-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5613-1 advisory.

It was discovered that Vim was not properly performing bounds checks when executing spell suggestion commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0943)

It was discovered that Vim was using freed memory when dealing with regular expressions through its old regular expression engine. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution. (CVE-2022-1154)

It was discovered that Vim was not properly performing checks on name of lambda functions. An attacker could possibly use this issue to cause a denial of service. This issue affected only Ubuntu 22.04 LTS.

(CVE-2022-1420)

It was discovered that Vim was incorrectly performing bounds checks when processing invalid commands with composing characters in Ex mode. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1616)

It was discovered that Vim was not properly processing latin1 data when issuing Ex commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1619)

It was discovered that Vim was not properly performing memory management when dealing with invalid regular expression patterns in buffers. An attacker could possibly use this issue to cause a denial of service.

(CVE-2022-1620)

It was discovered that Vim was not properly processing invalid bytes when performing spell check operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1621)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5613-1>

Solution

Update the affected 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-2022-0943 |
| CVE | CVE-2022-1154 |
| CVE | CVE-2022-1420 |
| CVE | CVE-2022-1616 |
| CVE | CVE-2022-1619 |
| CVE | CVE-2022-1620 |
| CVE | CVE-2022-1621 |
| XREF | USN:5613-1 |

Plugin Information

Published: 2022/09/15, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.8
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.8
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.8

170010 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5801-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5801-1 advisory.

It was discovered that Vim makes illegal memory calls when pasting brackets in Ex mode. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. This issue affected only Ubuntu 20.04 and 22.04 (CVE-2022-0392)

It was discovered that Vim makes illegal memory calls when making certain retab calls. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. (CVE-2022-0417)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5801-1>

Solution

Update the affected 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-2022-0392 |
| CVE | CVE-2022-0417 |
| XREF | USN:5801-1 |

Plugin Information

Published: 2023/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.11
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.11
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.11

173831 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5995-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5995-1 advisory.

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-0413, CVE-2022-1629, CVE-2022-1674, CVE-2022-1733, CVE-2022-1735, CVE-2022-1785, CVE-2022-1796, CVE-2022-1851, CVE-2022-1898, CVE-2022-1942, CVE-2022-1968, CVE-2022-2124, CVE-2022-2125, CVE-2022-2126, CVE-2022-2129, CVE-2022-2175, CVE-2022-2183, CVE-2022-2206, CVE-2022-2304, CVE-2022-2345, CVE-2022-2581)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1720, CVE-2022-2571, CVE-2022-2845, CVE-2022-2849, CVE-2022-2923)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-1927, CVE-2022-2344)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-2946)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-2980)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5995-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-0413 |
| CVE | CVE-2022-1629 |
| CVE | CVE-2022-1674 |
| CVE | CVE-2022-1720 |
| CVE | CVE-2022-1733 |
| CVE | CVE-2022-1735 |
| CVE | CVE-2022-1785 |
| CVE | CVE-2022-1796 |
| CVE | CVE-2022-1851 |
| CVE | CVE-2022-1898 |
| CVE | CVE-2022-1927 |
| CVE | CVE-2022-1942 |
| CVE | CVE-2022-1968 |
| CVE | CVE-2022-2124 |
| CVE | CVE-2022-2125 |
| CVE | CVE-2022-2126 |
| CVE | CVE-2022-2129 |
| CVE | CVE-2022-2175 |
| CVE | CVE-2022-2183 |
| CVE | CVE-2022-2206 |
| CVE | CVE-2022-2304 |
| CVE | CVE-2022-2344 |
| CVE | CVE-2022-2345 |
| CVE | CVE-2022-2571 |
| CVE | CVE-2022-2581 |
| CVE | CVE-2022-2845 |
| CVE | CVE-2022-2849 |
| CVE | CVE-2022-2923 |
| CVE | CVE-2022-2946 |
| CVE | CVE-2022-2980 |
| XREF | IAVB:2022-B-0049-S |
| XREF | USN:5995-1 |

Plugin Information

Published: 2023/04/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.13
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5

- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.13
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.13

165205 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Wayland vulnerability (USN-5614-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5614-1 advisory.

It was discovered that Wayland incorrectly handled reference counting certain objects. An attacker could use this issue to cause Wayland to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5614-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3782 |
| XREF | USN:5614-1 |

Plugin Information

Published: 2022/09/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libwayland-client0_1.18.0-1
- Fixed package : libwayland-client0_1.18.0-1ubuntu0.1
- Installed package : libwayland-cursor0_1.18.0-1
- Fixed package : libwayland-cursor0_1.18.0-1ubuntu0.1
- Installed package : libwayland-egl1_1.18.0-1
- Fixed package : libwayland-egl1_1.18.0-1ubuntu0.1
- Installed package : libwayland-server0_1.18.0-1
- Fixed package : libwayland-server0_1.18.0-1ubuntu0.1

163035 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerabilities (USN-5510-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5510-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5510-1>

Solution

Update the affected 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-2022-2319 |
| CVE | CVE-2022-2320 |
| XREF | USN:5510-1 |

Plugin Information

Published: 2022/07/12, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.3
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.3
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.3
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.3
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.3

171088 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerability (USN-5846-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5846-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5846-1>

Solution

Update the affected 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
XREF

CVE-2023-0494
USN:5846-1

Plugin Information

Published: 2023/02/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.6
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.6
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.6
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.6
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.6

173648 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerability (USN-5986-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5986-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5986-1>

Solution

Update the affected 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-2023-1393
XREF USN:5986-1

Plugin Information

Published: 2023/03/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.8

- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.8

- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.8

- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.8

- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.8
```

160318 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5397-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5397-1 advisory.

Patrick Monnerat discovered that curl incorrectly handled certain OAuth2. An attacker could possibly use this issue to access sensitive information. (CVE-2022-22576)

Harry Sintonen discovered that curl incorrectly handled certain requests. An attacker could possibly use this issue to expose sensitive information. (CVE-2022-27774, CVE-2022-27775, CVE-2022-27776)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5397-1>

Solution

Update the affected packages.

Risk Factor

Medium

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)

References

| | |
|------|----------------------|
| CVE | CVE-2022-22576 |
| CVE | CVE-2022-27774 |
| CVE | CVE-2022-27775 |
| CVE | CVE-2022-27776 |
| XREF | USN:5397-1 |
| XREF | CEA-ID:CEA-2022-0026 |

Plugin Information

Published: 2022/04/28, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.10
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.10

161058 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5412-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5412-1 advisory.

Axel Chong discovered that curl incorrectly handled percent-encoded URL separators. A remote attacker could possibly use this issue to trick curl into using the wrong URL and bypass certain checks or filters.

This issue only affected Ubuntu 22.04 LTS. (CVE-2022-27780)

Florian Kohnhuser discovered that curl incorrectly handled returning a TLS server's certificate chain details. A remote attacker could possibly use this issue to cause curl to stop responding, resulting in a denial of service. (CVE-2022-27781)

Harry Sintonen discovered that curl incorrectly reused a previous connection when certain options had been changed, contrary to expectations. (CVE-2022-27782)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5412-1>

Solution

Update the affected 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

6.7 (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

II

References

| | |
|------|--------------------|
| CVE | CVE-2022-27780 |
| CVE | CVE-2022-27781 |
| CVE | CVE-2022-27782 |
| XREF | USN:5412-1 |
| XREF | IAVA:2022-A-0224-S |

Plugin Information

Published: 2022/05/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.11
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.11

160308 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : networkd-dispatcher vulnerabilities (USN-5395-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5395-1 advisory.

It was discovered that networkd-dispatcher incorrectly handled internal scripts. A local attacker could possibly use this issue to cause a race condition, escalate privileges and execute arbitrary code.
(CVE-2022-29799, CVE-2022-29800)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5395-1>

Solution

Update the affected networkd-dispatcher package.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/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

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-29799
CVE CVE-2022-29800
XREF USN:5395-1

Plugin Information

Published: 2022/04/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : networkd-dispatcher_2.0.1-1
- Fixed package : networkd-dispatcher_2.1-2~ubuntu20.04.2

153367 - Ubuntu 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-5077-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5077-1 advisory.

Maik Mnch and Stephen Rttger discovered that Apport incorrectly handled certain information gathering operations. A local attacker could use this issue to gain read access to arbitrary files, possibly containing sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5077-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2021-3709 |
| CVE | CVE-2021-3710 |
| XREF | USN:5077-1 |

Plugin Information

Published: 2021/09/14, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.20
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.20
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.20
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.20

159059 - Ubuntu 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-5332-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5332-1 advisory.

Xiang Li, Baojun Liu, Chaoyi Lu, and Changgen Zou discovered that Bind incorrectly handled certain bogus NS records when using forwarders. A remote attacker could possibly use this issue to manipulate cache results. (CVE-2021-25220)

It was discovered that Bind incorrectly handled certain crafted TCP streams. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. This issue only affected Ubuntu 21.10. (CVE-2022-0396)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5332-1>

Solution

Update the affected packages.

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

|

References

| | |
|------|--------------------|
| CVE | CVE-2021-25220 |
| CVE | CVE-2022-0396 |
| XREF | USN:5332-1 |
| XREF | IAVA:2022-A-0122-S |

Plugin Information

Published: 2022/03/18, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.10
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.10
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.10

154704 - Ubuntu 18.04 LTS / 20.04 LTS : Bind vulnerability (USN-5126-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5126-1 advisory.

Kishore Kumar Kothapalli discovered that Bind incorrectly handled the lame cache when processing responses. A remote attacker could possibly use this issue to cause Bind to consume resources, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5126-1>

Solution

Update the affected 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: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

|

References

| | |
|------|--------------------|
| CVE | CVE-2021-25219 |
| XREF | USN:5126-1 |
| XREF | IAVA:2021-A-0525-S |

Plugin Information

Published: 2021/10/28, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bind9-dnsutils_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-dnsutils_1:9.16.1-0ubuntu2.9
- Installed package : bind9-host_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-host_1:9.16.1-0ubuntu2.9
- Installed package : bind9-libs_1:9.16.1-0ubuntu2.2
- Fixed package : bind9-libs_1:9.16.1-0ubuntu2.9

[155687 - Ubuntu 18.04 LTS / 20.04 LTS : BlueZ vulnerabilities \(USN-5155-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5155-1 advisory.

It was discovered that BlueZ incorrectly handled the Discoverable status when a device is powered down.

This could result in devices being powered up discoverable, contrary to expectations. This issue only affected Ubuntu 20.04 LTS, Ubuntu 21.04, and Ubuntu 21.10. (CVE-2021-3658)

It was discovered that BlueZ incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause BlueZ to consume resources, leading to a denial of service.

(CVE-2021-41229)

It was discovered that the BlueZ gatt server incorrectly handled disconnects. A remote attacker could possibly use this issue to cause BlueZ to crash, leading to a denial of service. (CVE-2021-43400)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5155-1>

Solution

Update the affected 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-2021-3658 |
| CVE | CVE-2021-41229 |

CVE-2021-43400
XREF USN:5155-1

Plugin Information

Published: 2021/11/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.4
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.4
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.4
- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.4

155939 - Ubuntu 18.04 LTS / 20.04 LTS : BusyBox vulnerabilities (USN-5179-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5179-1 advisory.

It was discovered that BusyBox incorrectly handled certain malformed gzip archives. If a user or automated system were tricked into processing a specially crafted gzip archive, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2021-28831)

It was discovered that BusyBox incorrectly handled certain malformed LZMA archives. If a user or automated system were tricked into processing a specially crafted LZMA archive, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly leak sensitive information.
(CVE-2021-42374)

Vera Mens, Uri Katz, Tal Keren, Sharon Brzinov, and Shachar Menashe discovered that BusyBox incorrectly handled certain awk patterns. If a user or automated system were tricked into processing a specially crafted awk pattern, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5179-1>

Solution

Update the affected 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/Vl:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:P/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

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

References

| | |
|------|----------------|
| CVE | CVE-2021-28831 |
| CVE | CVE-2021-42374 |
| CVE | CVE-2021-42378 |
| CVE | CVE-2021-42379 |
| CVE | CVE-2021-42380 |
| CVE | CVE-2021-42381 |
| CVE | CVE-2021-42382 |
| CVE | CVE-2021-42384 |
| CVE | CVE-2021-42385 |
| CVE | CVE-2021-42386 |
| XREF | USN:5179-1 |

Plugin Information

Published: 2021/12/08, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : busybox-initramfs_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-initramfs_1:1.30.1-4ubuntu6.4
- Installed package : busybox-static_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-static_1:1.30.1-4ubuntu6.4

140736 - Ubuntu 18.04 LTS / 20.04 LTS : BusyBox vulnerability (USN-4531-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4531-1 advisory.

It was discovered that the BusyBox wget applet incorrectly validated SSL certificates. A remote attacker could possibly use this issue to intercept secure communications.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4531-1>

Solution

Update the affected packages.

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-2018-1000500

XREF

USN:4531-1

Plugin Information

Published: 2020/09/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : busybox-initramfs_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-initramfs_1:1.30.1-4ubuntu6.2
- Installed package : busybox-static_1:1.30.1-4ubuntu6.1
- Fixed package : busybox-static_1:1.30.1-4ubuntu6.2

158259 - Ubuntu 18.04 LTS / 20.04 LTS : Cyrus SASL vulnerability (USN-5301-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5301-1 advisory.

It was discovered that the Cyrus SASL SQL plugin incorrectly handled SQL input. A remote attacker could use this issue to execute arbitrary SQL commands.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5301-1>

Solution

Update the affected 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

7.7 (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
XREF USN:5301-1

Plugin Information

Published: 2022/02/22, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libsasl2-2_2.1.27+dfsg-2
- Fixed package : libsasl2-2_2.1.27+dfsg-2ubuntu0.1
- Installed package : libsasl2-modules_2.1.27+dfsg-2
- Fixed package : libsasl2-modules_2.1.27+dfsg-2ubuntu0.1

- Installed package : libsasl2-modules-db_2.1.27+dfsg-2
- Fixed package : libsasl2-modules-db_2.1.27+dfsg-2ubuntu0.1

149527 - Ubuntu 18.04 LTS / 20.04 LTS : DjVuLibre vulnerabilities (USN-4957-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4957-1 advisory.

It was discovered that DjVuLibre incorrectly handled certain memory operations. If a user or automated system were tricked into processing a specially crafted DjVu file, a remote attacker could cause applications to hang or crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4957-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-3500 |
| CVE | CVE-2021-32490 |
| CVE | CVE-2021-32491 |
| CVE | CVE-2021-32492 |
| CVE | CVE-2021-32493 |
| XREF | USN:4957-1 |

Plugin Information

Published: 2021/05/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libdjvulibre-text_3.5.27.1-14build1
- Fixed package : libdjvulibre-text_3.5.27.1-14ubuntu0.1
- Installed package : libdjvulibre21_3.5.27.1-14build1
- Fixed package : libdjvulibre21_3.5.27.1-14ubuntu0.1

150143 - Ubuntu 18.04 LTS / 20.04 LTS : Dnsmasq vulnerability (USN-4976-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4976-1 advisory.

Petr Mensik discovered that Dnsmasq incorrectly randomized source ports in certain configurations. A remote attacker could possibly use this issue to facilitate DNS cache poisoning attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4976-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.6 (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:P/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3448 |
| XREF | USN:4976-1 |

Plugin Information

Published: 2021/06/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dnsmasq-base_2.80-1.1ubuntu1
- Fixed package : dnsmasq-base_2.80-1.1ubuntu1.4

150152 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4978-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4978-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, re-enable camera devices without an additional permission prompt, spoof the browser UI, or execute arbitrary code.
(CVE-2021-29959, CVE-2021-29961, CVE-2021-29966, CVE-2021-29967)

It was discovered that filenames printed from private browsing mode were incorrectly retained in preferences. A local attacker could potentially exploit this to obtain sensitive information.
(CVE-2021-29960)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4978-1>

Solution

Update the affected 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-2021-29959 |
| CVE | CVE-2021-29960 |
| CVE | CVE-2021-29961 |
| CVE | CVE-2021-29966 |
| CVE | CVE-2021-29967 |
| XREF | USN:4978-1 |

Plugin Information

Published: 2021/06/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_89.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_89.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_89.0+build2-0ubuntu0.20.04.2

151800 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5011-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5011-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, overlay text over another domain, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5011-1>

Solution

Update the affected 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

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-2021-29970 |
| CVE | CVE-2021-29972 |
| CVE | CVE-2021-29974 |
| CVE | CVE-2021-29975 |
| CVE | CVE-2021-29976 |
| CVE | CVE-2021-29977 |
| CVE | CVE-2021-30547 |
| XREF | USN:5011-1 |
| XREF | IAVA:2021-A-0309-S |
| XREF | IAVA:2021-A-0293-S |

Plugin Information

Published: 2021/07/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_90.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_90.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_90.0+build1-0ubuntu0.20.04.1

[152508 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities \(USN-5037-1\)](#)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5037-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5037-1>**Solution**

Update the affected 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

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-2021-29980 |
| CVE | CVE-2021-29981 |
| CVE | CVE-2021-29982 |
| CVE | CVE-2021-29984 |
| CVE | CVE-2021-29985 |
| CVE | CVE-2021-29986 |
| CVE | CVE-2021-29987 |
| CVE | CVE-2021-29988 |
| CVE | CVE-2021-29989 |
| CVE | CVE-2021-29990 |
| XREF | USN:5037-1 |

Plugin Information

Published: 2021/08/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_91.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_91.0+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_91.0+build2-0ubuntu0.20.04.1

153183 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5074-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5074-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass mixed content blocking, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5074-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-38491 |
| CVE | CVE-2021-38493 |
| CVE | CVE-2021-38494 |
| XREF | USN:5074-1 |
| XREF | IAVA:2021-A-0405-S |

Plugin Information

Published: 2021/09/09, Modified: 2025/03/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_92.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_92.0+build3-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_92.0+build3-0ubuntu0.20.04.1

153925 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5107-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5107-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof another origin, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5107-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-32810 |
| CVE | CVE-2021-38496 |
| CVE | CVE-2021-38497 |
| CVE | CVE-2021-38498 |
| CVE | CVE-2021-38499 |
| CVE | CVE-2021-38500 |
| CVE | CVE-2021-38501 |
| XREF | USN:5107-1 |
| XREF | IAVA:2021-A-0461-S |
| XREF | IAVA:2021-A-0450-S |

Plugin Information

Published: 2021/10/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_93.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_93.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_93.0+build1-0ubuntu0.20.04.1

155970 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5186-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5186-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct spoofing attacks, bypass CSP restrictions, or execute arbitrary code.
(CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43546)

A security issue was discovered with the handling of WebExtension permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to create and install a service worker that wouldn't be uninstalled with the extension. (CVE-2021-43540)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5186-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-43536 |
| CVE | CVE-2021-43537 |
| CVE | CVE-2021-43538 |
| CVE | CVE-2021-43539 |
| CVE | CVE-2021-43540 |
| CVE | CVE-2021-43541 |
| CVE | CVE-2021-43542 |
| CVE | CVE-2021-43543 |
| CVE | CVE-2021-43545 |
| CVE | CVE-2021-43546 |
| XREF | USN:5186-1 |
| XREF | IAVA:2021-A-0569-S |

Plugin Information

Published: 2021/12/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_95.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_95.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_95.0+build1-0ubuntu0.20.04.1

159593 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5370-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5370-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, execute script unexpectedly, obtain sensitive information, conduct spoofing attacks, or execute arbitrary code.
(CVE-2022-1097, CVE-2022-24713, CVE-2022-28281, CVE-2022-28282, CVE-2022-28284, CVE-2022-28285, CVE-2022-28286, CVE-2022-28288, CVE-2022-28289)

A security issue was discovered with the sourceMapURL feature of devtools. An attacker could potentially exploit this to include local files that should have been inaccessible. (CVE-2022-28283)

It was discovered that selecting text caused Firefox to crash in some circumstances. An attacker could potentially exploit this to cause a denial of service. (CVE-2022-28287)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5370-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-1097 |
| CVE | CVE-2022-24713 |
| CVE | CVE-2022-28281 |
| CVE | CVE-2022-28282 |
| CVE | CVE-2022-28283 |
| CVE | CVE-2022-28284 |
| CVE | CVE-2022-28285 |
| CVE | CVE-2022-28286 |
| CVE | CVE-2022-28287 |
| CVE | CVE-2022-28288 |
| CVE | CVE-2022-28289 |
| XREF | USN:5370-1 |
| XREF | IAVA:2022-A-0134-S |

Plugin Information

Published: 2022/04/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_99.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_99.0+build2-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_99.0+build2-0ubuntu0.20.04.2

149409 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerability (USN-4942-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4942-1 advisory.

A race condition was discovered in Web Render Components. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit this to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4942-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-29952 |
| XREF | USN:4942-1 |

Plugin Information

Published: 2021/05/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_88.0.1+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_88.0.1+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_88.0.1+build1-0ubuntu0.20.04.2

152681 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerability (USN-5047-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5047-1 advisory.

It was discovered that Firefox could be made to incorrectly accept newlines in HTTP/3 response headers. If a user were tricked into opening a specially crafted website, an attacker could exploit this to conduct header splitting attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5047-1>

Solution

Update the affected 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:H/A:N)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/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

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-29991 |
| XREF | USN:5047-1 |
| XREF | IAVA:2021-A-0386-S |

Plugin Information

Published: 2021/08/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_91.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_91.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_91.0.1+build1-0ubuntu0.20.04.1

140179 - Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-4481-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4481-1 advisory.

It was discovered that FreeRDP incorrectly handled certain memory operations. A remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4481-1>

Solution

Update the affected 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:L/I:N/A:L)

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:N/A:P)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-11095 |
| CVE | CVE-2020-11096 |
| CVE | CVE-2020-11097 |
| CVE | CVE-2020-11098 |
| CVE | CVE-2020-11099 |
| CVE | CVE-2020-15103 |
| CVE | CVE-2020-4030 |
| CVE | CVE-2020-4031 |
| CVE | CVE-2020-4032 |
| CVE | CVE-2020-4033 |
| XREF | USN:4481-1 |

Plugin Information

Published: 2020/09/02, Modified: 2025/05/27

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.1
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.1
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.1

155681 - Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-5154-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5154-1 advisory.

It was discovered that FreeRDP incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-41159)

It was discovered that FreeRDP incorrectly handled certain connections. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-41160)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5154-1>

Solution

Update the affected 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-2021-41159 |
| CVE | CVE-2021-41160 |
| XREF | USN:5154-1 |

Plugin Information

Published: 2021/11/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libfreerdp-client2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.20.04.2
- Installed package : libfreerdp2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.20.04.2
- Installed package : libwinpr2-2_2.1.1+dfsg1-0ubuntu0.20.04.1
- Fixed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.20.04.2

142369 - Ubuntu 18.04 LTS / 20.04 LTS : GDM vulnerability (USN-4614-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4614-1 advisory.

Kevin Backhouse discovered that GDM incorrectly launched the initial setup tool when the accountsservice daemon was not reachable. A local attacker able to cause accountsservice to crash or stop responding could trick GDM into launching the initial setup tool and create a privileged user.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4614-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2020-16125
XREF USN:4614-1

Plugin Information

Published: 2020/11/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gdm3_3.34.1-1ubuntu1
- Fixed package : gdm3_3.36.3-0ubuntu0.20.04.2
- Installed package : gir1.2-gdm-1.0_3.34.1-1ubuntu1
- Fixed package : gir1.2-gdm-1.0_3.36.3-0ubuntu0.20.04.2
- Installed package : libgdm1_3.34.1-1ubuntu1
- Fixed package : libgdm1_3.36.3-0ubuntu0.20.04.2

154413 - Ubuntu 18.04 LTS / 20.04 LTS : GNU binutils vulnerabilities (USN-5124-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5124-1 advisory.

It was discovered that GNU binutils incorrectly handled certain hash lookups. An attacker could use this issue to cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-16592)

It was discovered that GNU binutils incorrectly handled certain corrupt DWARF debug sections. An attacker could possibly use this issue to cause GNU binutils to consume memory, resulting in a denial of service.
(CVE-2021-3487)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5124-1>

Solution

Update the affected 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-2020-16592
CVE-2021-3487
XREF USN:5124-1

Plugin Information

Published: 2021/10/26, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.3

- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.3

- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.3

- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.3

- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.3

- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.3
```

153143 - Ubuntu 18.04 LTS / 20.04 LTS : GNU cpio vulnerability (USN-5064-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5064-1 advisory.

Maverick Chung and Qiaoyi Fang discovered that cpio incorrectly handled certain pattern files. A remote attacker could use this issue to cause cpio to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5064-1>

Solution

Update the affected cpio and / or cpio-win32 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-2021-38185 |
| XREF | USN:5064-1 |

Plugin Information

Published: 2021/09/08, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : cpio_2.13+dfsg-2
- Fixed package : cpio_2.13+dfsg-2ubuntu0.3

156645 - Ubuntu 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-5224-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5224-1 advisory.

It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5224-1>

Solution

Update the affected 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-2021-45944 |
| CVE | CVE-2021-45949 |
| XREF | USN:5224-1 |

Plugin Information

Published: 2022/01/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.5
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.5
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.5
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.5

172631 - Ubuntu 18.04 LTS / 20.04 LTS : Kerberos vulnerabilities (USN-5959-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5959-1 advisory.

It was discovered that Kerberos incorrectly handled memory when processing KDC data, which could lead to a NULL pointer dereference. An attacker could possibly use this issue to cause a denial of service or have other unspecified impacts. (CVE-2021-36222, CVE-2021-37750)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5959-1>

Solution

Update the affected 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

6.5 (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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-36222 |
| CVE | CVE-2021-37750 |
| XREF | USN:5959-1 |

Plugin Information

Published: 2023/03/16, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.3
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.3
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.3
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.3
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.3

167060 - Ubuntu 18.04 LTS / 20.04 LTS : LibRaw vulnerabilities (USN-5715-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5715-1 advisory.

It was discovered that LibRaw incorrectly handled photo files. If a user or automated system were tricked into processing a specially crafted photo file, a remote attacker could cause applications linked against LibRaw to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5715-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-15503 |
| CVE | CVE-2020-35530 |
| CVE | CVE-2020-35531 |
| CVE | CVE-2020-35532 |
| CVE | CVE-2020-35533 |
| XREF | USN:5715-1 |

Plugin Information

Published: 2022/11/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libraw19_0.19.5-1ubuntu1
- Fixed package : libraw19_0.19.5-1ubuntu1.1

164944 - Ubuntu 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5523-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5523-2 advisory.

USN-5523-1 fixed several vulnerabilities in LibTIFF. This update provides the fixes for CVE-2022-0907, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924 and CVE-2022-22844 for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5523-2>

Solution

Update the affected 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-2022-0907 |
| CVE | CVE-2022-0908 |
| CVE | CVE-2022-0909 |
| CVE | CVE-2022-0924 |
| CVE | CVE-2022-22844 |
| XREF | USN:5523-2 |

Plugin Information

Published: 2022/09/12, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.4
```

153447 - Ubuntu 18.04 LTS / 20.04 LTS : Libgcrypt vulnerabilities (USN-5080-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5080-1 advisory.

It was discovered that Libgcrypt incorrectly handled ElGamal encryption. An attacker could possibly use this issue to recover sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5080-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/NC:H/VI:H/V/A: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-33560 |
| CVE | CVE-2021-40528 |
| XREF | USN:5080-1 |

Plugin Information

Published: 2021/09/16, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : libgcrypt20_1.8.5-5ubuntu1
- Fixed package : libgcrypt20_1.8.5-5ubuntu1.1

158938 - Ubuntu 18.04 LTS / 20.04 LTS : LibreOffice vulnerability (USN-5330-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5330-1 advisory.

It was discovered that LibreOffice incorrectly handled digital signatures. An attacker could possibly use this issue to create a specially crafted document that would display a validly signed indicator, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5330-1>

Solution

Update the affected 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-2021-25636 |
| XREF | USN:5330-1 |

Plugin Information

Published: 2022/03/15, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.4
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.4

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libuno-purvenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purvenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.4
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.4
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.4
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.4
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.4

140723 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4525-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4525-1 advisory.

It was discovered that the AMD Cryptographic Coprocessor device driver in the Linux kernel did not properly deallocate memory in some situations. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-18808)

It was discovered that the Conexant 23885 TV card device driver for the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19054)

It was discovered that the VFIO PCI driver in the Linux kernel did not properly handle attempts to access disabled memory spaces. A local attacker could use this to cause a denial of service (system crash).

(CVE-2020-12888)

It was discovered that the state of network RNG in the Linux kernel was potentially observable. A remote attacker could use this to expose sensitive information. (CVE-2020-16166)

It was discovered that the NFS client implementation in the Linux kernel did not properly perform bounds checking before copying security labels in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-25212)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4525-1>

Solution

Update the affected kernel package.

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

6.1 (CVSS:3.0/E:U/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

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

References

| | |
|------|----------------|
| CVE | CVE-2019-18808 |
| CVE | CVE-2019-19054 |
| CVE | CVE-2020-12888 |
| CVE | CVE-2020-16166 |
| CVE | CVE-2020-25212 |
| XREF | USN:4525-1 |

Plugin Information

Published: 2020/09/22, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-48-generic for this advisory.
```

141451 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4576-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4576-1 advisory.

Hadar Manor discovered that the DCCP protocol implementation in the Linux kernel improperly handled socket reuse, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-16119)

Jay Shin discovered that the ext4 file system implementation in the Linux kernel did not properly handle directory access with broken indexing, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-14314)

David Alan Gilbert discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation in some circumstances. A local attacker could use this to cause a denial of service. (CVE-2020-14385)

Giuseppe Scrivano discovered that the overlay file system in the Linux kernel did not properly perform permission checks in some situations. A local attacker could possibly use this to bypass intended restrictions and gain read access to restricted files. (CVE-2020-16120)

It was discovered that a race condition existed in the hugetlb sysctl implementation in the Linux kernel.
A privileged attacker could use this to cause a denial of service (system crash). (CVE-2020-25285)

It was discovered that the block layer subsystem in the Linux kernel did not properly handle zero-length requests. A local attacker could use this to cause a denial of service. (CVE-2020-25641)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4576-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-14314 |
| CVE | CVE-2020-14385 |
| CVE | CVE-2020-16119 |
| CVE | CVE-2020-16120 |
| CVE | CVE-2020-25285 |
| CVE | CVE-2020-25641 |
| XREF | USN:4576-1 |

Plugin Information

Published: 2020/10/14, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-51-generic for this advisory.

148034 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4887-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4887-1 advisory.

De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker could use this to expose sensitive information (kernel memory) or possibly execute arbitrary code.
(CVE-2021-3444)

Adam Nichols discovered that heap overflows existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.
(CVE-2021-27365)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly compute a speculative execution limit on pointer arithmetic in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-27171)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly apply speculative execution limits on some pointer types. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-27170)

Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did not properly restrict access to iSCSI transport handles. A local attacker could use this to cause a denial of service or expose sensitive information (kernel pointer addresses). (CVE-2021-27363)

Adam Nichols discovered that an out-of-bounds read existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2021-27364)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4887-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-27170 |
| CVE | CVE-2020-27171 |
| CVE | CVE-2021-3444 |
| CVE | CVE-2021-27363 |
| CVE | CVE-2021-27364 |
| CVE | CVE-2021-27365 |
| XREF | USN:4887-1 |

Plugin Information

Published: 2021/03/24, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-70-generic for this advisory.
```

148497 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4909-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4909-1 advisory.

Loris Reiff discovered that the BPF implementation in the Linux kernel did not properly validate attributes in the getsockopt BPF hook. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-20194)

Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H. Schuhmehl discovered that the Xen paravirtualization backend in the Linux kernel did not properly propagate errors to frontend drivers in some situations. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2021-26930)

Jan Beulich discovered that multiple Xen backends in the Linux kernel did not properly handle certain error conditions under paravirtualization. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2021-26931)

It was discovered that the network block device (nbd) driver in the Linux kernel contained a use-after-free vulnerability during device setup. A local attacker with access to the nbd device could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3348)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4909-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-3348 |
| CVE | CVE-2021-20194 |
| CVE | CVE-2021-26930 |
| CVE | CVE-2021-26931 |
| XREF | USN:4909-1 |

Plugin Information

Published: 2021/04/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-71-generic for this advisory.
```

152639 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5045-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5045-1 advisory.

Norbert Slusarek discovered that the CAN broadcast manger (bcm) protocol implementation in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-34693)

It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device initialization failure, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-3564)

It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device detach events, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-3573)

It was discovered that the NFC implementation in the Linux kernel did not properly handle failed connect events leading to a NULL pointer dereference. A local attacker could use this to cause a denial of service. (CVE-2021-3587)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5045-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.8 (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-2021-3564 |
| CVE | CVE-2021-3573 |
| CVE | CVE-2021-34693 |
| XREF | USN:5045-1 |

Plugin Information

Published: 2021/08/18, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-81-generic for this advisory.

154278 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5116-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5116-1 advisory.

It was discovered that a race condition existed in the Atheros Ath9k WiFi driver in the Linux kernel. An attacker could possibly use this to expose sensitive information (WiFi network traffic). (CVE-2020-3702)

Alois Wohlschlager discovered that the overlay file system in the Linux kernel did not restrict private clones in some situations. An attacker could use this to expose sensitive information. (CVE-2021-3732)

It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly compute the access permissions for shadow pages in some situations. A local attacker could use this to cause a denial of service. (CVE-2021-38198)

It was discovered that the Xilinx 10/100 Ethernet Lite device driver in the Linux kernel could report pointer addresses in some situations. An attacker could use this information to ease the exploitation of another vulnerability. (CVE-2021-38205)

It was discovered that the ext4 file system in the Linux kernel contained a race condition when writing xattr to an inode. A local attacker could use this to cause a denial of service or possibly gain administrative privileges. (CVE-2021-40490)

It was discovered that the 6pack network protocol driver in the Linux kernel did not properly perform validation checks. A privileged attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-42008)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5116-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

References

| | |
|------|----------------|
| CVE | CVE-2020-3702 |
| CVE | CVE-2021-3732 |
| CVE | CVE-2021-38198 |
| CVE | CVE-2021-38205 |
| CVE | CVE-2021-40490 |
| CVE | CVE-2021-42008 |
| XREF | USN:5116-1 |

Plugin Information

Published: 2021/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-89-generic for this advisory.

154980 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5137-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5137-1 advisory.

It was discovered that the f2fs file system in the Linux kernel did not properly validate metadata in some situations. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-19449)

It was discovered that the Infiniband RDMA userspace connection manager implementation in the Linux kernel contained a race condition leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-36385)

Wolfgang Frisch discovered that the ext4 file system implementation in the Linux kernel contained an integer overflow when handling metadata inode extents. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2021-3428)

Benedict Schlueter discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side-channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-34556)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side-channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-35477)

It was discovered that the btrfs file system in the Linux kernel did not properly handle removing a non-existent device id. An attacker with CAP_SYS_ADMIN could use this to cause a denial of service.
(CVE-2021-3739)

It was discovered that the Qualcomm IPC Router protocol implementation in the Linux kernel did not properly validate metadata in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2021-3743)

It was discovered that the virtual terminal (vt) device implementation in the Linux kernel contained a race condition in its ioctl handling that led to an out-of-bounds read vulnerability. A local attacker could possibly use this to expose sensitive information. (CVE-2021-3753)

It was discovered that the Linux kernel did not properly account for the memory usage of certain IPC objects. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3759)

It was discovered that the Aspeed Low Pin Count (LPC) Bus Controller implementation in the Linux kernel did not properly perform boundary checks in some situations, allowing out-of-bounds write access. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. In Ubuntu, this issue only affected systems running armhf kernels. (CVE-2021-42252)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5137-1>

Solution

Update the affected kernel package.

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:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2019-19449 |
| CVE | CVE-2020-36385 |
| CVE | CVE-2021-3428 |
| CVE | CVE-2021-3739 |
| CVE | CVE-2021-3743 |
| CVE | CVE-2021-3753 |
| CVE | CVE-2021-3759 |
| CVE | CVE-2021-34556 |
| CVE | CVE-2021-35477 |
| CVE | CVE-2021-42252 |
| XREF | USN:5137-1 |

Plugin Information

Published: 2021/11/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-90-generic for this advisory.
```

155749 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5163-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5163-1 advisory.

Ilja Van Sprundel discovered that the SCTP implementation in the Linux kernel did not properly perform size validations on incoming packets in some situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2021-3655)

It was discovered that the Option USB High Speed Mobile device driver in the Linux kernel did not properly handle error conditions. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-37159)

It was discovered that the AMD Cryptographic Coprocessor (CCP) driver in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3744, CVE-2021-3764)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5163-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.8 (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)

References

| | |
|------|----------------|
| CVE | CVE-2021-3655 |
| CVE | CVE-2021-3744 |
| CVE | CVE-2021-3764 |
| CVE | CVE-2021-37159 |
| XREF | USN:5163-1 |

Plugin Information

Published: 2021/12/01, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-91-generic for this advisory.

158737 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5318-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5318-1 advisory.

Nick Gregory discovered that the Linux kernel incorrectly handled network offload functionality. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-25636)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by ARM to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-23960)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by Intel to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-0001, CVE-2022-0002)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5318-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-0001 |
| CVE | CVE-2022-0002 |
| CVE | CVE-2022-23960 |
| CVE | CVE-2022-25636 |
| XREF | USN:5318-1 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2022/03/09, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-104-generic for this advisory.
```

159373 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5358-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5358-1 advisory.

It was discovered that the network traffic control implementation in the Linux kernel contained a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1055)

It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-27666)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5358-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-1055 |
| CVE | CVE-2022-27666 |
| XREF | USN:5358-1 |

Exploitable With

CANVAS (true)

Plugin Information

Published: 2022/03/31, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-107-generic for this advisory.

161063 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5415-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5415-1 advisory.

Jeremy Cline discovered a use-after-free in the nouveau graphics driver of the Linux kernel during device removal. A privileged or physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-27820)

Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-26401)

David Bouman discovered that the netfilter subsystem in the Linux kernel did not initialize memory in some situations. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2022-1016)

It was discovered that the MMC/SD subsystem in the Linux kernel did not properly handle read errors from SD cards in certain situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-20008)

It was discovered that the USB gadget subsystem in the Linux kernel did not properly validate interface descriptor requests. An attacker could possibly use this to cause a denial of service (system crash).

(CVE-2022-25258)

It was discovered that the Remote NDIS (RNDIS) USB gadget implementation in the Linux kernel did not properly validate the size of the RNDIS_MSG_SET command. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-25375)

It was discovered that the ST21NFCA NFC driver in the Linux kernel did not properly validate the size of certain data in EVT_TRANSACTION events. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-26490)

It was discovered that the Xilinx USB2 device gadget driver in the Linux kernel did not properly validate endpoint indices from the host. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-27223)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5415-1>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-27820 |
| CVE | CVE-2021-26401 |
| CVE | CVE-2022-1016 |
| CVE | CVE-2022-20008 |
| CVE | CVE-2022-25258 |
| CVE | CVE-2022-25375 |
| CVE | CVE-2022-26490 |
| CVE | CVE-2022-27223 |
| XREF | USN:5415-1 |

Plugin Information

Published: 2022/05/12, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-110-generic for this advisory.

163113 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5514-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5514-1 advisory.

It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1195)

Duoming Zhou discovered that the AX.25 amateur radio protocol implementation in the Linux kernel did not handle detach events properly in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1199)

Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel during device detach operations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1204)

Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel, leading to use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1205)

Yongkang Jia discovered that the KVM hypervisor implementation in the Linux kernel did not properly handle guest TLB mapping invalidation requests in some situations. An attacker in a guest VM could use this to cause a denial of service (system crash) in the host OS. (CVE-2022-1789)

Minh Yuan discovered that the floppy driver in the Linux kernel contained a race condition in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-33981)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5514-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2022-1195 |
| CVE | CVE-2022-1199 |
| CVE | CVE-2022-1204 |
| CVE | CVE-2022-1205 |
| CVE | CVE-2022-1789 |
| CVE | CVE-2022-33981 |
| XREF | USN:5514-1 |

Plugin Information

Published: 2022/07/14, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-122-generic for this advisory.

168348 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5756-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5756-1 advisory.

Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)

It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3524)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3564)

It was discovered that the ISDN implementation of the Linux kernel contained a use-after-free vulnerability. A privileged user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3565)

It was discovered that the TCP implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3566)

It was discovered that the IPv6 implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3567)

It was discovered that the Realtek RTL8152 USB Ethernet adapter driver in the Linux kernel did not properly handle certain error conditions. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3594)

It was discovered that a null pointer dereference existed in the NILFS2 file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3621)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5756-1>

Solution

Update the affected kernel package.

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-2022-3524 |
| CVE | CVE-2022-3564 |
| CVE | CVE-2022-3565 |
| CVE | CVE-2022-3566 |
| CVE | CVE-2022-3567 |
| CVE | CVE-2022-3594 |
| CVE | CVE-2022-3621 |
| CVE | CVE-2022-42703 |
| XREF | USN:5756-1 |

Plugin Information

Published: 2022/12/02, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-135-generic for this advisory.

169689 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory.

It was discovered that a race condition existed in the Android Binder IPC subsystem in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-20421)

David Leadbeater discovered that the netfilter IRC protocol tracking implementation in the Linux Kernel incorrectly handled certain message payloads in some situations. A remote attacker could possibly use this to cause a denial of service or bypass firewall filtering. (CVE-2022-2663)

It was discovered that the Intel 740 frame buffer driver in the Linux kernel contained a divide by zero vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3061)

It was discovered that the sound subsystem in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3303)

Gwnaun Jung discovered that the SFB packet scheduling implementation in the Linux kernel contained a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3586)

It was discovered that the NILFS2 file system implementation in the Linux kernel did not properly deallocate memory in certain error conditions. An attacker could

use this to cause a denial of service (memory exhaustion). (CVE-2022-3646)

Hyunwoo Kim discovered that an integer overflow vulnerability existed in the PXA3xx graphics driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash).
(CVE-2022-39842)

It was discovered that a race condition existed in the EFI capsule loader driver in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-40307)

Zheng Wang and Zhuorao Yang discovered that the RealTek RTL8712U wireless driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-4095)

It was discovered that the USB monitoring (usbmon) component in the Linux kernel did not properly set permissions on memory mapped in to user space processes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43750)

Jann Horn discovered a race condition existed in the Linux kernel when unmapping VMAs in certain situations, resulting in possible use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-39188)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5791-1>

Solution

Update the affected kernel package.

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-2022-2663 |
| CVE | CVE-2022-3061 |
| CVE | CVE-2022-3303 |
| CVE | CVE-2022-3586 |
| CVE | CVE-2022-3646 |
| CVE | CVE-2022-39188 |
| CVE | CVE-2022-4095 |
| CVE | CVE-2022-20421 |
| CVE | CVE-2022-39842 |
| CVE | CVE-2022-40307 |
| CVE | CVE-2022-43750 |
| XREF | USN:5791-1 |

Plugin Information

Published: 2023/01/07, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-136-generic for this advisory.

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory.

It was discovered that the Traffic-Control Index (TCINDEX) implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-1281)

Jiasheng Jiang discovered that the HSA Linux kernel driver for AMD Radeon GPU devices did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3108)

It was discovered that the infrared transceiver USB driver did not properly handle USB control messages. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3903)

Haowei Yan discovered that a race condition existed in the Layer 2 Tunneling Protocol (L2TP) implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-4129)

It was discovered that the Human Interface Device (HID) support driver in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1073)

It was discovered that a memory leak existed in the SCTP protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2023-1074)

Lianhui Tang discovered that the MPLS implementation in the Linux kernel did not properly handle certain sysctl allocation failure conditions, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-26545)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6027-1>

Solution

Update the affected kernel package.

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-2022-3108 |
| CVE | CVE-2022-3903 |
| CVE | CVE-2022-4129 |
| CVE | CVE-2023-1073 |
| CVE | CVE-2023-1074 |
| CVE | CVE-2023-1281 |
| CVE | CVE-2023-26545 |
| XREF | USN:6027-1 |

Plugin Information

Published: 2023/04/19, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-147-generic for this advisory.

176228 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory.

Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-3707)

Jordy Zomer and Alexandra Sandulescu discovered that the Linux kernel did not properly implement speculative execution barriers in usercopy functions in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2023-0459)

It was discovered that the TLS subsystem in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1075)

It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-1078)

Xingyuan Mo discovered that the x86 KVM implementation in the Linux kernel did not properly initialize some data structures. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2023-1513)

It was discovered that a use-after-free vulnerability existed in the iSCSI TCP implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash).

(CVE-2023-2162)

It was discovered that the NET/ROM protocol implementation in the Linux kernel contained a race condition in some situations, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32269)

Duoming Zhou discovered that a race condition existed in the infrared receiver/transceiver driver in the Linux kernel, leading to a use-after- free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-1118)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6094-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|-----|---------------|
| CVE | CVE-2022-3707 |
| CVE | CVE-2023-0459 |
| CVE | CVE-2023-1075 |

| | |
|------|----------------|
| CVE | CVE-2023-1078 |
| CVE | CVE-2023-1118 |
| CVE | CVE-2023-1513 |
| CVE | CVE-2023-2162 |
| CVE | CVE-2023-32269 |
| XREF | USN:6094-1 |

Plugin Information

Published: 2023/05/23, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-149-generic for this advisory.

176564 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory.

Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32233)

Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-31436)

Reima Ishii discovered that the nested KVM implementation for Intel x86 processors in the Linux kernel did not properly validate control registers in certain situations. An attacker in a guest VM could use this to cause a denial of service (guest crash). (CVE-2023-30456)

It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform data buffer size validation in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1380)

Jean-Baptiste Cayrou discovered that the shiftfs file system in the Ubuntu Linux kernel contained a race condition when handling inode locking in some situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2612)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6131-1>

Solution

Update the affected kernel package.

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-2023-1380 |
| CVE | CVE-2023-2612 |
| CVE | CVE-2023-30456 |
| CVE | CVE-2023-31436 |
| CVE | CVE-2023-32233 |
| XREF | USN:6131-1 |

Exploitable With

Core Impact (true)

Plugin Information

Published: 2023/06/01, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-150-generic for this advisory.

191663 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6681-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6681-1 advisory.

Wenqing Liu discovered that the f2fs file system implementation in the Linux kernel did not properly validate inode types while performing garbage collection. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2021-44879)

It was discovered that the DesignWare USB3 for Qualcomm SoCs driver in the Linux kernel did not properly handle certain error conditions during device registration. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-22995)

Bien Pham discovered that the netfiler subsystem in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4244)

It was discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51779)

It was discovered that a race condition existed in the ATM (Asynchronous Transfer Mode) subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51780)

It was discovered that a race condition existed in the Rose X.25 protocol implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51782)

Alon Zahavi discovered that the NVMe-of/TCP subsystem of the Linux kernel did not properly handle connect command payloads in certain situations, leading to an out-of-bounds read vulnerability. A remote attacker could use this to expose sensitive information (kernel memory). (CVE-2023-6121)

It was discovered that the VirtIO subsystem in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to possibly expose sensitive information (kernel memory). (CVE-2024-0340)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6681-1>

Solution

Update the affected kernel package.

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

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-2021-44879 |
| CVE | CVE-2023-4244 |
| CVE | CVE-2023-6121 |
| CVE | CVE-2023-22995 |
| CVE | CVE-2023-51779 |
| CVE | CVE-2023-51780 |
| CVE | CVE-2023-51782 |
| CVE | CVE-2024-0340 |
| XREF | USN:6681-1 |

Plugin Information

Published: 2024/03/07, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-173-generic for this advisory.

192292 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6702-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6702-1 advisory.

It was discovered that the NVIDIA Tegra XUSB pad controller driver in the Linux kernel did not properly handle return values in certain error conditions. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-23000)

It was discovered that the ARM Mali Display Processor driver implementation in the Linux kernel did not properly handle certain error conditions. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-23004)

Notselwyn discovered that the netfilter subsystem in the Linux kernel did not properly handle verdict parameters in certain cases, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-1086)

It was discovered that a race condition existed in the SCSI Emulex LightPulse Fibre Channel driver in the Linux kernel when unregistering FCF and re-scanning an HBA FCF table, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-24855)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6702-1>

Solution

Update the affected kernel package.

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-2023-23000 |
| CVE | CVE-2023-23004 |
| CVE | CVE-2024-1086 |
| CVE | CVE-2024-24855 |
| XREF | USN:6702-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/06/20 |

Plugin Information

Published: 2024/03/20, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-174-generic for this advisory.

193081 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6726-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6726-1 advisory.

Pratyush Yadav discovered that the Xen network backend implementation in the Linux kernel did not properly handle zero length data request, leading to a null pointer dereference vulnerability. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2023-46838)

It was discovered that the IPv6 implementation of the Linux kernel did not properly manage route cache memory usage. A remote attacker could use this to cause a denial of service (memory exhaustion).

(CVE-2023-52340)

It was discovered that the device mapper driver in the Linux kernel did not properly validate target size during certain memory allocations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-52429, CVE-2024-23851)

Dan Carpenter discovered that the netfilter subsystem in the Linux kernel did not store data in properly sized memory locations. A local user could use this to cause a denial of service (system crash).

(CVE-2024-0607)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Architecture specifics;
- Cryptographic API;
- Android drivers;
- EDAC drivers;
- GPU drivers;
- Media drivers;

- MTD block device drivers;
- Network drivers;
- NVME drivers;
- TTY drivers;
- Userspace I/O drivers;
- F2FS file system;
- GFS2 file system;
- IPv6 Networking;
- AppArmor security module; (CVE-2023-52464, CVE-2023-52448, CVE-2023-52457, CVE-2023-52443, CVE-2023-52439, CVE-2023-52612, CVE-2024-26633, CVE-2024-26597, CVE-2023-52449, CVE-2023-52444, CVE-2023-52609, CVE-2023-52469, CVE-2023-52445, CVE-2023-52451, CVE-2023-52470, CVE-2023-52454, CVE-2023-52436, CVE-2023-52438)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6726-1>

Solution

Update the affected kernel package.

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-2023-46838 |
| CVE | CVE-2023-52340 |
| CVE | CVE-2023-52429 |
| CVE | CVE-2023-52436 |
| CVE | CVE-2023-52438 |
| CVE | CVE-2023-52439 |
| CVE | CVE-2023-52443 |
| CVE | CVE-2023-52444 |
| CVE | CVE-2023-52445 |
| CVE | CVE-2023-52448 |
| CVE | CVE-2023-52449 |
| CVE | CVE-2023-52451 |
| CVE | CVE-2023-52454 |
| CVE | CVE-2023-52457 |
| CVE | CVE-2023-52464 |
| CVE | CVE-2023-52469 |
| CVE | CVE-2023-52470 |
| CVE | CVE-2023-52609 |
| CVE | CVE-2023-52612 |
| CVE | CVE-2024-0607 |
| CVE | CVE-2024-23851 |
| CVE | CVE-2024-26597 |
| CVE | CVE-2024-26633 |
| XREF | USN:6726-1 |

Plugin Information

Published: 2024/04/09, Modified: 2025/03/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-176-generic for this advisory.

193596 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6741-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6741-1 advisory.

Daniele Antonioli discovered that the Secure Simple Pairing and Secure Connections pairing in the Bluetooth protocol could allow an unauthenticated user to complete authentication without pairing credentials. A physically proximate attacker placed between two Bluetooth devices could use this to subsequently impersonate one of the paired devices. (CVE-2023-24023)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- JFS file system;
- BPF subsystem;
- Netfilter; (CVE-2023-52603, CVE-2023-52600, CVE-2024-26581, CVE-2024-26589)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6741-1>

Solution

Update the affected kernel package.

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-2023-24023 |
| CVE | CVE-2023-52600 |
| CVE | CVE-2023-52603 |
| CVE | CVE-2024-26581 |
| CVE | CVE-2024-26589 |
| XREF | USN:6741-1 |

Plugin Information

Published: 2024/04/19, Modified: 2025/03/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-177-generic for this advisory.

195135 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6767-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6767-1 advisory.

Chenyuan Yang discovered that the RDS Protocol implementation in the Linux kernel contained an out-of-bounds read vulnerability. An attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-23849)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;
- PowerPC architecture;
- S390 architecture;
- Block layer subsystem;
- Android drivers;
- Hardware random number generator core;
- GPU drivers;
- Hardware monitoring drivers;
- I2C subsystem;
- IIO Magnetometer sensors drivers;
- InfiniBand drivers;
- Network drivers;
- PCI driver for MicroSemi Switchtec;
- PHY drivers;
- Ceph distributed file system;
- Ext4 file system;
- JFS file system;
- NILFS2 file system;
- Pstore file system;
- Core kernel;
- Memory management;
- CAN network layer;

- Networking core;
 - IPv4 networking;
 - Logical Link layer;
 - Netfilter;
 - NFC subsystem;
 - SMC sockets;
 - Sun RPC protocol;
 - TIPC protocol;
- Realtek audio codecs; (CVE-2024-26696, CVE-2023-52583, CVE-2024-26720, CVE-2023-52615, CVE-2023-52599, CVE-2023-52587, CVE-2024-26635, CVE-2024-26704, CVE-2024-26625, CVE-2024-26825, CVE-2023-52622, CVE-2023-52435, CVE-2023-52617, CVE-2023-52598, CVE-2024-26645, CVE-2023-52619, CVE-2024-26593, CVE-2024-26685, CVE-2023-52602, CVE-2023-52486, CVE-2024-26697, CVE-2024-26675, CVE-2024-26600, CVE-2023-52604, CVE-2024-26664, CVE-2024-26606, CVE-2023-52594, CVE-2024-26671, CVE-2024-26598, CVE-2024-26673, CVE-2024-26920, CVE-2024-26722, CVE-2023-52601, CVE-2024-26602, CVE-2023-52637, CVE-2023-52623, CVE-2024-26702, CVE-2023-52597, CVE-2024-26684, CVE-2023-52606, CVE-2024-26679, CVE-2024-26663, CVE-2024-26910, CVE-2024-26615, CVE-2023-52595, CVE-2023-52607, CVE-2024-26636)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6767-1>

Solution

Update the affected kernel package.

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-2023-52435 |
| CVE | CVE-2023-52486 |
| CVE | CVE-2023-52583 |
| CVE | CVE-2023-52587 |
| CVE | CVE-2023-52594 |
| CVE | CVE-2023-52595 |
| CVE | CVE-2023-52597 |
| CVE | CVE-2023-52598 |
| CVE | CVE-2023-52599 |
| CVE | CVE-2023-52601 |
| CVE | CVE-2023-52602 |
| CVE | CVE-2023-52604 |
| CVE | CVE-2023-52606 |
| CVE | CVE-2023-52607 |
| CVE | CVE-2023-52615 |
| CVE | CVE-2023-52617 |
| CVE | CVE-2023-52619 |
| CVE | CVE-2023-52622 |
| CVE | CVE-2023-52623 |
| CVE | CVE-2023-52637 |
| CVE | CVE-2024-23849 |
| CVE | CVE-2024-26593 |

| | |
|------|----------------|
| CVE | CVE-2024-26598 |
| CVE | CVE-2024-26600 |
| CVE | CVE-2024-26602 |
| CVE | CVE-2024-26606 |
| CVE | CVE-2024-26615 |
| CVE | CVE-2024-26625 |
| CVE | CVE-2024-26635 |
| CVE | CVE-2024-26636 |
| CVE | CVE-2024-26645 |
| CVE | CVE-2024-26663 |
| CVE | CVE-2024-26664 |
| CVE | CVE-2024-26671 |
| CVE | CVE-2024-26673 |
| CVE | CVE-2024-26675 |
| CVE | CVE-2024-26679 |
| CVE | CVE-2024-26684 |
| CVE | CVE-2024-26685 |
| CVE | CVE-2024-26696 |
| CVE | CVE-2024-26697 |
| CVE | CVE-2024-26702 |
| CVE | CVE-2024-26704 |
| CVE | CVE-2024-26720 |
| CVE | CVE-2024-26722 |
| CVE | CVE-2024-26825 |
| CVE | CVE-2024-26910 |
| CVE | CVE-2024-26920 |
| XREF | USN:6767-1 |

Plugin Information

Published: 2024/05/07, Modified: 2025/02/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-181-generic for this advisory.

197218 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6776-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6776-1 advisory.

Zheng Wang discovered that the Broadcom FullMAC WLAN driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-47233)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Networking core;
- IPv4 networking;
- MAC80211 subsystem;
- Tomoyo security module; (CVE-2024-26614, CVE-2023-52530, CVE-2024-26622)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6776-1>

Solution

Update the affected kernel package.

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-2023-47233 |
| CVE | CVE-2023-52530 |
| CVE | CVE-2024-26614 |
| CVE | CVE-2024-26622 |
| XREF | USN:6776-1 |

Plugin Information

Published: 2024/05/16, Modified: 2024/12/13

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-182-generic for this advisory.

200450 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6831-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6831-1 advisory.

It was discovered that the HugeTLB file system component of the Linux Kernel contained a NULL pointer dereference vulnerability. A privileged attacker could possibly use this to cause a denial of service.

(CVE-2024-0841)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;
- PowerPC architecture;
- x86 architecture;
- DMA engine subsystem;
- EFI core;
- GPU drivers;
- InfiniBand drivers;
- Multiple devices driver;
- Network drivers;
- Power supply drivers;

- TCM subsystem;
- Userspace I/O drivers;
- USB subsystem;
- Framebuffer layer;
- AFS file system;
- File systems infrastructure;
- BTRFS file system;
- Ext4 file system;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- L2TP protocol;
- MAC80211 subsystem;
- Netfilter;
- Netlink;

- Wireless networking; (CVE-2024-26748, CVE-2024-27417, CVE-2024-26840, CVE-2023-52504, CVE-2024-26790, CVE-2024-26763, CVE-2024-26805, CVE-2024-26773, CVE-2021-47063, CVE-2024-26791, CVE-2024-27413, CVE-2024-26788, CVE-2024-27405, CVE-2024-26845, CVE-2024-26766, CVE-2021-47070, CVE-2024-26839, CVE-2024-26712, CVE-2024-27412, CVE-2024-26752, CVE-2024-26778, CVE-2024-26735, CVE-2024-26736, CVE-2024-27410, CVE-2024-26779, CVE-2024-26804, CVE-2024-26749, CVE-2024-26793, CVE-2024-26764, CVE-2024-26751, CVE-2024-35811, CVE-2024-26835, CVE-2024-26772, CVE-2024-26777, CVE-2024-26688, CVE-2024-27416, CVE-2024-26801, CVE-2024-26733, CVE-2024-27414, CVE-2024-26754, CVE-2024-26848)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6831-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2021-47063 |
| CVE | CVE-2021-47070 |
| CVE | CVE-2023-52504 |
| CVE | CVE-2024-0841 |

CVE-CVE-2024-26688
CVE-CVE-2024-26712
CVE-CVE-2024-26733
CVE-CVE-2024-26735
CVE-CVE-2024-26736
CVE-CVE-2024-26748
CVE-CVE-2024-26749
CVE-CVE-2024-26751
CVE-CVE-2024-26752
CVE-CVE-2024-26754
CVE-CVE-2024-26763
CVE-CVE-2024-26764
CVE-CVE-2024-26766
CVE-CVE-2024-26772
CVE-CVE-2024-26773
CVE-CVE-2024-26777
CVE-CVE-2024-26778
CVE-CVE-2024-26779
CVE-CVE-2024-26788
CVE-CVE-2024-26790
CVE-CVE-2024-26791
CVE-CVE-2024-26793
CVE-CVE-2024-26801
CVE-CVE-2024-26804
CVE-CVE-2024-26805
CVE-CVE-2024-26835
CVE-CVE-2024-26839
CVE-CVE-2024-26840
CVE-CVE-2024-26845
CVE-CVE-2024-26848
CVE-CVE-2024-27405
CVE-CVE-2024-27410
CVE-CVE-2024-27412
CVE-CVE-2024-27413
CVE-CVE-2024-27414
CVE-CVE-2024-27416
CVE-CVE-2024-27417
CVE-CVE-2024-35811
XREF-USN:6831-1

Plugin Information

Published: 2024/06/12, Modified: 2024/12/23

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-186-generic for this advisory.

201871 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6868-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6868-1 advisory.

Sander Wiebing, Alvise de Faveri Tron, Herbert Bos, and Cristiano Giuffrida discovered that the Linux kernel mitigations for the initial Branch History Injection vulnerability (CVE-2022-0001) were insufficient for Intel processors. A local attacker could potentially use this to expose sensitive information. (CVE-2024-2201)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Netfilter; (CVE-2024-26925, CVE-2024-26643)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6868-1>

Solution

Update the affected kernel package.

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

4.8 (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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-2201 |
| CVE | CVE-2024-26643 |
| CVE | CVE-2024-26925 |
| XREF | USN:6868-1 |

Plugin Information

Published: 2024/07/04, Modified: 2025/03/19

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-187-generic for this advisory.

202292 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6896-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6896-1 advisory.

It was discovered that the ATA over Ethernet (AoE) driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6270)

It was discovered that the Atheros 802.11ac wireless driver did not properly validate certain data structures, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service. (CVE-2023-7042)

Yuxuan Hu discovered that the Bluetooth RFCOMM protocol driver in the Linux Kernel contained a race condition, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-22099)

Gui-Dong Han discovered that the software RAID driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. A privileged attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-23307)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel when modifying certain settings values through debugfs. A privileged local attacker could use this to cause a denial of service. (CVE-2024-24857, CVE-2024-24858, CVE-2024-24859)

Bai Jiaju discovered that the Xceive XC4000 silicon tuner device driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-24861)

Chenyuan Yang discovered that the Unsorted Block Images (UBI) flash device volume management subsystem did not properly validate logical eraseblock sizes in certain situations. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-25739)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the

following subsystems:

- x86 architecture;
- Block layer subsystem;
- Accessibility subsystem;
- ACPI drivers;
- Android drivers;
- Bluetooth drivers;
- Clock framework and drivers;
- Data acquisition framework and drivers;
- Cryptographic API;
- GPU drivers;
- HID subsystem;
- I2C subsystem;
- IRQ chip drivers;
- Multiple devices driver;
- Media drivers;
- VMware VMCI Driver;
- MMC subsystem;
- Network drivers;
- PCI subsystem;
- SCSI drivers;
- Freescale SoC drivers;
- SPI subsystem;
- Media staging drivers;
- TTY drivers;
- USB subsystem;
- VFIO drivers;
- Framebuffer layer;
- Xen hypervisor drivers;
- File systems infrastructure;
- BTRFS file system;
- Ext4 file system;
- FAT file system;
- NILFS2 file system;
- Diskquota system;
- SMB network file system;
- UBI file system;

- io_uring subsystem;
- BPF subsystem;
- Core kernel;
- Memory management;
- B.A.T.M.A.N. meshing protocol;
- Bluetooth subsystem;
- Networking core;
- HSR network protocol;
- IPv4 networking;
- IPv6 networking;
- MAC80211 subsystem;
- Netfilter;
- NET/ROM layer;
- NFC subsystem;
- Open vSwitch;
- Packet sockets;
- RDS protocol;
- Network traffic control;
- Sun RPC protocol;
- Unix domain sockets;
- ALSA SH drivers;
- USB sound devices;
- KVM core; (CVE-2024-35969, CVE-2024-35819, CVE-2024-26851, CVE-2024-26816, CVE-2024-26643, CVE-2023-52656, CVE-2024-27020, CVE-2024-35821, CVE-2024-35930, CVE-2024-35936, CVE-2024-27075, CVE-2024-26817, CVE-2024-26984, CVE-2024-35895, CVE-2024-35853, CVE-2024-27043, CVE-2024-35978, CVE-2024-35960, CVE-2024-26882, CVE-2024-35806, CVE-2024-35830, CVE-2024-26852, CVE-2024-35915, CVE-2024-36006, CVE-2024-35935, CVE-2024-26926, CVE-2024-35877, CVE-2024-27396, CVE-2024-26654, CVE-2024-27077, CVE-2024-27078, CVE-2024-27000, CVE-2024-35888, CVE-2024-27437, CVE-2024-26994, CVE-2024-26973, CVE-2024-26687, CVE-2024-26955, CVE-2024-26898, CVE-2024-26859, CVE-2023-52620, CVE-2024-35893, CVE-2024-26903, CVE-2024-26862, CVE-2024-35950, CVE-2023-52644, CVE-2024-26969, CVE-2024-27028, CVE-2024-35984, CVE-2024-36007, CVE-2024-35925, CVE-2024-36020, CVE-2024-26956, CVE-2024-35789, CVE-2024-26878, CVE-2024-35855, CVE-2024-35822, CVE-2023-52699, CVE-2024-27044, CVE-2024-27030, CVE-2024-27065, CVE-2024-26993, CVE-2024-27395, CVE-2024-27013, CVE-2024-35922, CVE-2024-26586, CVE-2024-36004, CVE-2024-35897, CVE-2024-35807, CVE-2024-26901, CVE-2024-27076, CVE-2023-52880, CVE-2022-48627, CVE-2024-26894, CVE-2023-52650, CVE-2024-27001, CVE-2024-26863, CVE-2024-26651, CVE-2024-35886, CVE-2024-35982, CVE-2024-26883, CVE-2024-26935, CVE-2024-27074, CVE-2024-35849, CVE-2024-35955, CVE-2024-26965, CVE-2024-35898, CVE-2024-26855, CVE-2024-35933, CVE-2024-35823, CVE-2024-35815, CVE-2024-26880, CVE-2024-26874, CVE-2024-26642, CVE-2024-26937, CVE-2024-35854, CVE-2024-35997, CVE-2024-27059, CVE-2024-26812, CVE-2024-26999, CVE-2024-26923, CVE-2024-26934, CVE-2024-27024, CVE-2024-27419, CVE-2024-35847, CVE-2024-26974, CVE-2024-26875, CVE-2024-35805, CVE-2024-27008, CVE-2024-26889, CVE-2024-27053, CVE-2024-27388, CVE-2024-26981, CVE-2024-26976, CVE-2024-35973, CVE-2024-35852, CVE-2024-35809, CVE-2024-27004, CVE-2024-26884, CVE-2024-35899, CVE-2024-26931, CVE-2024-35813, CVE-2024-26922, CVE-2024-26957, CVE-2024-35944, CVE-2024-27038, CVE-2024-35910, CVE-2024-26925, CVE-2024-26820, CVE-2024-26857, CVE-2024-26828, CVE-2024-35825, CVE-2024-26813, CVE-2024-27046, CVE-2024-26810, CVE-2024-27436, CVE-2024-27073, CVE-2024-35828, CVE-2024-35900, CVE-2024-26966)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6896-1>

Solution

Update the affected kernel package.

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-2022-48627
CVE CVE-2023-6270
CVE CVE-2023-7042
CVE CVE-2023-52620
CVE CVE-2023-52644
CVE CVE-2023-52650
CVE CVE-2023-52656
CVE CVE-2023-52699
CVE CVE-2023-52880
CVE CVE-2024-22099
CVE CVE-2024-23307
CVE CVE-2024-24857
CVE CVE-2024-24858
CVE CVE-2024-24859
CVE CVE-2024-24861
CVE CVE-2024-25739
CVE CVE-2024-26586
CVE CVE-2024-26642
CVE CVE-2024-26643
CVE CVE-2024-26651
CVE CVE-2024-26654
CVE CVE-2024-26687
CVE CVE-2024-26810
CVE CVE-2024-26812
CVE CVE-2024-26813
CVE CVE-2024-26816
CVE CVE-2024-26817
CVE CVE-2024-26820
CVE CVE-2024-26828
CVE CVE-2024-26851
CVE CVE-2024-26852
CVE CVE-2024-26855
CVE CVE-2024-26857
CVE CVE-2024-26859
CVE CVE-2024-26862
CVE CVE-2024-26863
CVE CVE-2024-26874
CVE CVE-2024-26875
CVE CVE-2024-26878
CVE CVE-2024-26880
CVE CVE-2024-26882
CVE CVE-2024-26883
CVE CVE-2024-26884
CVE CVE-2024-26889
CVE CVE-2024-26894
CVE CVE-2024-26898
CVE CVE-2024-26901
CVE CVE-2024-26903
CVE CVE-2024-26922
CVE CVE-2024-26923
CVE CVE-2024-26925
CVE CVE-2024-26926
CVE CVE-2024-26931
CVE CVE-2024-26934
CVE CVE-2024-26935
CVE CVE-2024-26937
CVE CVE-2024-26955
CVE CVE-2024-26956
CVE CVE-2024-26957
CVE CVE-2024-26965
CVE CVE-2024-26966
CVE CVE-2024-26969

CVE-CVE-2024-26973
CVE-CVE-2024-26974
CVE-CVE-2024-26976
CVE-CVE-2024-26981
CVE-CVE-2024-26984
CVE-CVE-2024-26993
CVE-CVE-2024-26994
CVE-CVE-2024-26999
CVE-CVE-2024-27000
CVE-CVE-2024-27001
CVE-CVE-2024-27004
CVE-CVE-2024-27008
CVE-CVE-2024-27013
CVE-CVE-2024-27020
CVE-CVE-2024-27024
CVE-CVE-2024-27028
CVE-CVE-2024-27030
CVE-CVE-2024-27038
CVE-CVE-2024-27043
CVE-CVE-2024-27044
CVE-CVE-2024-27046
CVE-CVE-2024-27053
CVE-CVE-2024-27059
CVE-CVE-2024-27065
CVE-CVE-2024-27073
CVE-CVE-2024-27074
CVE-CVE-2024-27075
CVE-CVE-2024-27076
CVE-CVE-2024-27077
CVE-CVE-2024-27078
CVE-CVE-2024-27388
CVE-CVE-2024-27395
CVE-CVE-2024-27396
CVE-CVE-2024-27419
CVE-CVE-2024-27436
CVE-CVE-2024-27437
CVE-CVE-2024-35789
CVE-CVE-2024-35805
CVE-CVE-2024-35806
CVE-CVE-2024-35807
CVE-CVE-2024-35809
CVE-CVE-2024-35813
CVE-CVE-2024-35815
CVE-CVE-2024-35819
CVE-CVE-2024-35821
CVE-CVE-2024-35822
CVE-CVE-2024-35823
CVE-CVE-2024-35825
CVE-CVE-2024-35828
CVE-CVE-2024-35830
CVE-CVE-2024-35847
CVE-CVE-2024-35849
CVE-CVE-2024-35852
CVE-CVE-2024-35853
CVE-CVE-2024-35854
CVE-CVE-2024-35855
CVE-CVE-2024-35877
CVE-CVE-2024-35886
CVE-CVE-2024-35888
CVE-CVE-2024-35893
CVE-CVE-2024-35895
CVE-CVE-2024-35897
CVE-CVE-2024-35898
CVE-CVE-2024-35899
CVE-CVE-2024-35900
CVE-CVE-2024-35910
CVE-CVE-2024-35915
CVE-CVE-2024-35922
CVE-CVE-2024-35925
CVE-CVE-2024-35930
CVE-CVE-2024-35933
CVE-CVE-2024-35935
CVE-CVE-2024-35936
CVE-CVE-2024-35944
CVE-CVE-2024-35950
CVE-CVE-2024-35955
CVE-CVE-2024-35960
CVE-CVE-2024-35969
CVE-CVE-2024-35973
CVE-CVE-2024-35978
CVE-CVE-2024-35982
CVE-CVE-2024-35984

| | |
|------|----------------|
| CVE | CVE-2024-35997 |
| CVE | CVE-2024-36004 |
| CVE | CVE-2024-36006 |
| CVE | CVE-2024-36007 |
| CVE | CVE-2024-36020 |
| XREF | USN:6896-1 |

Plugin Information

Published: 2024/07/12, Modified: 2024/12/31

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-189-generic for this advisory.

204835 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6924-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6924-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM SCMI message protocol;
- InfiniBand drivers;
- TTY drivers;
- TLS protocol; (CVE-2024-26584, CVE-2024-36016, CVE-2024-26585, CVE-2021-47131, CVE-2024-26907, CVE-2022-48655, CVE-2024-26583)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6924-1>

Solution

Update the affected kernel package.

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-2021-47131 |
| CVE | CVE-2022-48655 |

| | |
|------|----------------|
| CVE | CVE-2024-26583 |
| CVE | CVE-2024-26584 |
| CVE | CVE-2024-26585 |
| CVE | CVE-2024-26907 |
| CVE | CVE-2024-36016 |
| XREF | USN:6924-1 |

Plugin Information

Published: 2024/07/29, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-190-generic for this advisory.

206077 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6973-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6973-1 advisory.

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel, leading to a null pointer dereference vulnerability. A privileged local attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-24860)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- SuperH RISC architecture;
- MMC subsystem;
- Network drivers;
- SCSI drivers;
- GFS2 file system;
- IPv4 networking;
- IPv6 networking;
- HD-audio driver; (CVE-2024-26830, CVE-2024-39484, CVE-2024-36901, CVE-2024-26929, CVE-2024-26921, CVE-2021-46926, CVE-2023-52629, CVE-2023-52760)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6973-1>

Solution

Update the affected kernel package.

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-2021-46926 |
| CVE | CVE-2023-52629 |
| CVE | CVE-2023-52760 |
| CVE | CVE-2024-24860 |
| CVE | CVE-2024-26830 |
| CVE | CVE-2024-26921 |
| CVE | CVE-2024-26929 |
| CVE | CVE-2024-36901 |
| CVE | CVE-2024-39484 |
| XREF | USN:6973-1 |

Plugin Information

Published: 2024/08/21, Modified: 2025/01/07

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-193-generic for this advisory.

207398 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7022-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7022-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- GPU drivers;
 - Modular ISDN driver;
 - MMC subsystem;
 - SCSI drivers;
 - F2FS file system;
 - GFS2 file system;
 - Netfilter;
 - RxRPC session sockets;
- Integrity Measurement Architecture(IMA) framework; (CVE-2021-47188, CVE-2024-27012, CVE-2024-42228, CVE-2022-48791, CVE-2024-39494, CVE-2022-48863, CVE-2024-26787, CVE-2024-42160, CVE-2024-38570, CVE-2024-26677)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7022-1>

Solution

Update the affected kernel package.

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-2021-47188 |
| CVE | CVE-2022-48791 |
| CVE | CVE-2022-48863 |
| CVE | CVE-2024-26677 |
| CVE | CVE-2024-26787 |
| CVE | CVE-2024-27012 |
| CVE | CVE-2024-38570 |
| CVE | CVE-2024-39494 |
| CVE | CVE-2024-42160 |
| CVE | CVE-2024-42228 |
| XREF | USN:7022-1 |

Plugin Information

Published: 2024/09/18, Modified: 2024/09/18

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-196-generic for this advisory.

209164 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7073-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7073-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Watchdog drivers;
- Netfilter;
- Memory management;
- Network traffic control; (CVE-2024-27397, CVE-2024-38630, CVE-2024-45016, CVE-2024-26960)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7073-1>

Solution

Update the affected kernel package.

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-2024-26960 |
| CVE | CVE-2024-27397 |
| CVE | CVE-2024-38630 |
| CVE | CVE-2024-45016 |
| XREF | USN:7073-1 |

Plugin Information

Published: 2024/10/17, Modified: 2024/10/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-198-generic for this advisory.

212722 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7159-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7159-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;
- ARM64 architecture;
- S390 architecture;
- x86 architecture;
- Power management core;
- GPU drivers;
- InfiniBand drivers;
- Network drivers;
- S/390 drivers;

- TTY drivers;
 - BTRFS file system;
 - EROFS file system;
 - F2FS file system;
 - File systems infrastructure;
 - BPF subsystem;
 - Socket messages infrastructure;
 - Bluetooth subsystem;
 - Ethernet bridge;
 - Networking core;
 - IPv4 networking;
- SELinux security module; (CVE-2022-48938, CVE-2024-42156, CVE-2024-36953, CVE-2024-38538, CVE-2021-47501, CVE-2024-42068, CVE-2024-26947, CVE-2024-46724, CVE-2024-36968, CVE-2023-52497, CVE-2024-35951, CVE-2023-52488, CVE-2024-44940, CVE-2022-48733, CVE-2023-52498, CVE-2022-48943, CVE-2024-35904, CVE-2024-42077, CVE-2024-36938, CVE-2023-52639, CVE-2024-42240, CVE-2024-44942, CVE-2021-47076)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7159-1>

Solution

Update the affected kernel package.

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-2021-47076 |
| CVE | CVE-2021-47501 |
| CVE | CVE-2022-48733 |
| CVE | CVE-2022-48938 |
| CVE | CVE-2022-48943 |
| CVE | CVE-2023-52488 |
| CVE | CVE-2023-52497 |
| CVE | CVE-2023-52498 |
| CVE | CVE-2023-52639 |
| CVE | CVE-2024-26947 |
| CVE | CVE-2024-35904 |
| CVE | CVE-2024-35951 |
| CVE | CVE-2024-36938 |
| CVE | CVE-2024-36953 |
| CVE | CVE-2024-36968 |
| CVE | CVE-2024-38538 |
| CVE | CVE-2024-42068 |
| CVE | CVE-2024-42077 |
| CVE | CVE-2024-42156 |

| | |
|------|----------------|
| CVE | CVE-2024-42240 |
| CVE | CVE-2024-44940 |
| CVE | CVE-2024-44942 |
| CVE | CVE-2024-46724 |
| XREF | USN:7159-1 |

Plugin Information

Published: 2024/12/12, Modified: 2024/12/12

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-202-generic for this advisory.

213100 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7173-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7173-1 advisory.

Ziming Zhang discovered that the DRM driver for VMware Virtual GPU did not properly handle certain error conditions, leading to a NULL pointer dereference. A local attacker could possibly trigger this vulnerability to cause a denial of service. (CVE-2022-38096)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- GPU drivers;
- Network drivers;
- SCSI subsystem;
- Ext4 file system;
- Bluetooth subsystem;
- Memory management;
- Amateur Radio drivers;
- Network traffic control;
- Sun RPC protocol;
- VMware vSockets driver; (CVE-2023-52821, CVE-2024-40910, CVE-2024-43892, CVE-2024-49967, CVE-2024-50264, CVE-2024-36952, CVE-2024-38553, CVE-2021-47101, CVE-2021-47001, CVE-2024-35965, CVE-2024-35963, CVE-2024-35966, CVE-2024-35967, CVE-2024-53057, CVE-2024-38597)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7173-1>

Solution

Update the affected kernel package.

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-2021-47001 |
| CVE | CVE-2021-47101 |
| CVE | CVE-2022-38096 |
| CVE | CVE-2023-52821 |
| CVE | CVE-2024-35963 |
| CVE | CVE-2024-35965 |
| CVE | CVE-2024-35966 |
| CVE | CVE-2024-35967 |
| CVE | CVE-2024-36952 |
| CVE | CVE-2024-38553 |
| CVE | CVE-2024-38597 |
| CVE | CVE-2024-40910 |
| CVE | CVE-2024-43892 |
| CVE | CVE-2024-49967 |
| CVE | CVE-2024-50264 |
| CVE | CVE-2024-53057 |
| XREF | USN:7173-1 |

Plugin Information

Published: 2024/12/17, Modified: 2024/12/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-204-generic for this advisory.

214732 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7234-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7234-1 advisory.

Ye Zhang and Nicolas Wu discovered that the io_uring subsystem in the Linux kernel did not properly handle locking for rings with IOPOLL, leading to a double-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-21400)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- TTY drivers;
- Netfilter;
- Network traffic control;
- VMware vSockets driver; (CVE-2024-53141, CVE-2024-53103, CVE-2024-40967, CVE-2024-53164)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7234-1>

Solution

Update the affected kernel package.

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-2023-21400 |
| CVE | CVE-2024-40967 |
| CVE | CVE-2024-53103 |
| CVE | CVE-2024-53141 |
| CVE | CVE-2024-53164 |
| XREF | USN:7234-1 |

Plugin Information

Published: 2025/01/28, Modified: 2025/01/28

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-205-generic for this advisory.

233669 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7391-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7391-1 advisory.

Chenyuan Yang discovered that the CEC driver driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-23848)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- PowerPC architecture;
- S390 architecture;
- SuperH RISC architecture;
- User-Mode Linux (UML);
- x86 architecture;
- Cryptographic API;
- Virtio block driver;
- Data acquisition framework and drivers;

- Hardware crypto device drivers;
- DMA engine subsystem;
- EDAC drivers;
- ARM SCPI message protocol;
- GPIO subsystem;
- GPU drivers;
- HID subsystem;
- Microsoft Hyper-V drivers;
- I3C subsystem;
- IIO ADC drivers;
- IIO subsystem;
- InfiniBand drivers;
- LED subsystem;
- Multiple devices driver;
- Media drivers;
- Multifunction device drivers;
- MMC subsystem;
- MTD block device drivers;
- Network drivers;
- Mellanox network drivers;
- NVME drivers;
- PCI subsystem;
- Pin controllers subsystem;
- x86 platform drivers;
- Real Time Clock drivers;
- SCSI subsystem;
- SuperH / SH-Mobile drivers;
- QCOM SoC drivers;
- SPI subsystem;
- USB Gadget drivers;
- USB Serial drivers;
- USB Type-C Port Controller Manager driver;
- VFIO drivers;
- Framebuffer layer;
- Xen hypervisor drivers;
- BTRFS file system;
- Ext4 file system;

- F2FS file system;
- GFS2 file system;
- File systems infrastructure;
- JFFS2 file system;
- JFS file system;
- Network file system (NFS) client;
- Network file system (NFS) server daemon;
- NILFS2 file system;
- Overlay file system;
- Proc file system;
- Diskquota system;
- SMB network file system;
- UBI file system;
- Timer subsystem;
- VLANs driver;
- LAPB network protocol;
- Kernel init infrastructure;
- BPF subsystem;
- Kernel CPU control infrastructure;
- Tracing infrastructure;
- Memory management;
- 9P file system network protocol;
- Bluetooth subsystem;
- CAN network layer;
- Networking core;
- DCCP (Datagram Congestion Control Protocol);
- IEEE802154.4 network protocol;
- IPv4 networking;
- IPv6 networking;
- IEEE 802.15.4 subsystem;
- Netfilter;
- Netlink;
- NET/ROM layer;
- Packet sockets;
- Network traffic control;
- SCTP protocol;
- Sun RPC protocol;

- TIPC protocol;
- eXpress Data Path;
- SELinux security module;
- USB sound devices; (CVE-2024-53172, CVE-2024-56572, CVE-2024-56739, CVE-2024-56643, CVE-2024-53131, CVE-2024-57904, CVE-2024-53145, CVE-2024-57908, CVE-2024-53155, CVE-2024-56691, CVE-2024-57901, CVE-2024-56595, CVE-2024-55916, CVE-2024-50051, CVE-2024-49936, CVE-2024-57900, CVE-2024-53239, CVE-2024-53142, CVE-2024-57889, CVE-2024-53217, CVE-2024-56619, CVE-2025-21653, CVE-2024-53140, CVE-2024-53130, CVE-2024-43098, CVE-2024-56746, CVE-2024-56650, CVE-2024-56723, CVE-2024-56558, CVE-2024-57884, CVE-2024-56601, CVE-2024-56581, CVE-2024-57906, CVE-2024-57948, CVE-2024-49996, CVE-2024-56598, CVE-2025-21638, CVE-2024-49925, CVE-2024-56767, CVE-2024-53127, CVE-2024-53181, CVE-2024-53194, CVE-2024-57902, CVE-2024-56630, CVE-2024-56567, CVE-2024-56602, CVE-2024-56562, CVE-2024-56596, CVE-2024-56570, CVE-2024-56670, CVE-2024-53135, CVE-2024-56629, CVE-2024-56769, CVE-2024-56637, CVE-2024-56681, CVE-2024-57910, CVE-2024-57892, CVE-2024-56574, CVE-2024-53121, CVE-2024-56532, CVE-2025-21689, CVE-2024-53156, CVE-2024-57912, CVE-2024-56597, CVE-2025-21640, CVE-2024-53690, CVE-2024-56548, CVE-2024-56633, CVE-2024-43900, CVE-2024-56631, CVE-2021-47219, CVE-2024-56659, CVE-2024-53158, CVE-2025-21639, CVE-2024-53136, CVE-2024-56615, CVE-2024-56586, CVE-2024-57946, CVE-2024-57911, CVE-2025-21699, CVE-2025-21664, CVE-2024-53174, CVE-2024-53184, CVE-2024-53138, CVE-2024-53680, CVE-2024-56593, CVE-2024-56644, CVE-2024-56720, CVE-2024-53197, CVE-2024-57802, CVE-2024-53157, CVE-2024-56756, CVE-2024-53171, CVE-2024-57931, CVE-2024-56600, CVE-2024-53112, CVE-2024-56770, CVE-2024-53214, CVE-2024-57849, CVE-2024-57890, CVE-2024-56634, CVE-2024-44938, CVE-2024-53183, CVE-2025-21697, CVE-2024-57929, CVE-2024-53165, CVE-2024-53161, CVE-2024-53150, CVE-2024-56606, CVE-2024-56748, CVE-2024-48881, CVE-2024-56594, CVE-2024-56645, CVE-2024-56781, CVE-2024-56531, CVE-2024-56605, CVE-2024-56779, CVE-2025-21678, CVE-2024-53227, CVE-2024-56688, CVE-2024-56576, CVE-2024-56587, CVE-2024-53124, CVE-2024-49884, CVE-2024-57850, CVE-2024-56569, CVE-2024-53148, CVE-2025-21694, CVE-2024-56700, CVE-2024-53173, CVE-2024-53198, CVE-2024-52332, CVE-2024-47707, CVE-2024-56539, CVE-2024-56704, CVE-2024-56747, CVE-2025-21687, CVE-2024-56690, CVE-2022-49034, CVE-2024-57938, CVE-2024-57951, CVE-2024-38588, CVE-2024-56603, CVE-2024-57807, CVE-2024-56780, CVE-2024-57922, CVE-2024-56642, CVE-2024-57913, CVE-2024-53146, CVE-2024-56614, CVE-2024-56694, CVE-2024-56724)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7391-1>

Solution

Update the affected kernel package.

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

7.2 (CVSS:3.0/E:F/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

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

References

| | |
|-----|----------------|
| CVE | CVE-2021-47219 |
| CVE | CVE-2022-49034 |
| CVE | CVE-2024-23848 |
| CVE | CVE-2024-38588 |
| CVE | CVE-2024-43098 |
| CVE | CVE-2024-43900 |
| CVE | CVE-2024-44938 |
| CVE | CVE-2024-47707 |
| CVE | CVE-2024-48881 |
| CVE | CVE-2024-49884 |
| CVE | CVE-2024-49925 |
| CVE | CVE-2024-49936 |
| CVE | CVE-2024-49996 |
| CVE | CVE-2024-50051 |
| CVE | CVE-2024-52332 |
| CVE | CVE-2024-53112 |
| CVE | CVE-2024-53121 |
| CVE | CVE-2024-53124 |
| CVE | CVE-2024-53127 |
| CVE | CVE-2024-53130 |

CVE-CVE-2024-53131
CVE-CVE-2024-53135
CVE-CVE-2024-53136
CVE-CVE-2024-53138
CVE-CVE-2024-53140
CVE-CVE-2024-53142
CVE-CVE-2024-53145
CVE-CVE-2024-53146
CVE-CVE-2024-53148
CVE-CVE-2024-53150
CVE-CVE-2024-53155
CVE-CVE-2024-53156
CVE-CVE-2024-53157
CVE-CVE-2024-53158
CVE-CVE-2024-53161
CVE-CVE-2024-53165
CVE-CVE-2024-53171
CVE-CVE-2024-53172
CVE-CVE-2024-53173
CVE-CVE-2024-53174
CVE-CVE-2024-53181
CVE-CVE-2024-53183
CVE-CVE-2024-53184
CVE-CVE-2024-53194
CVE-CVE-2024-53197
CVE-CVE-2024-53198
CVE-CVE-2024-53214
CVE-CVE-2024-53217
CVE-CVE-2024-53227
CVE-CVE-2024-53239
CVE-CVE-2024-53680
CVE-CVE-2024-53690
CVE-CVE-2024-55916
CVE-CVE-2024-56531
CVE-CVE-2024-56532
CVE-CVE-2024-56539
CVE-CVE-2024-56548
CVE-CVE-2024-56558
CVE-CVE-2024-56562
CVE-CVE-2024-56567
CVE-CVE-2024-56569
CVE-CVE-2024-56570
CVE-CVE-2024-56572
CVE-CVE-2024-56574
CVE-CVE-2024-56576
CVE-CVE-2024-56581
CVE-CVE-2024-56586
CVE-CVE-2024-56587
CVE-CVE-2024-56593
CVE-CVE-2024-56594
CVE-CVE-2024-56595
CVE-CVE-2024-56596
CVE-CVE-2024-56597
CVE-CVE-2024-56598
CVE-CVE-2024-56600
CVE-CVE-2024-56601
CVE-CVE-2024-56602
CVE-CVE-2024-56603
CVE-CVE-2024-56605
CVE-CVE-2024-56606
CVE-CVE-2024-56614
CVE-CVE-2024-56615
CVE-CVE-2024-56619
CVE-CVE-2024-56629
CVE-CVE-2024-56630
CVE-CVE-2024-56631
CVE-CVE-2024-56633
CVE-CVE-2024-56634
CVE-CVE-2024-56637
CVE-CVE-2024-56642
CVE-CVE-2024-56643
CVE-CVE-2024-56644
CVE-CVE-2024-56645
CVE-CVE-2024-56650
CVE-CVE-2024-56659
CVE-CVE-2024-56670
CVE-CVE-2024-56681
CVE-CVE-2024-56688
CVE-CVE-2024-56690
CVE-CVE-2024-56691
CVE-CVE-2024-56694
CVE-CVE-2024-56700

| | |
|------|---------------------------------|
| CVE | CVE-2024-56704 |
| CVE | CVE-2024-56720 |
| CVE | CVE-2024-56723 |
| CVE | CVE-2024-56724 |
| CVE | CVE-2024-56739 |
| CVE | CVE-2024-56746 |
| CVE | CVE-2024-56747 |
| CVE | CVE-2024-56748 |
| CVE | CVE-2024-56756 |
| CVE | CVE-2024-56767 |
| CVE | CVE-2024-56769 |
| CVE | CVE-2024-56770 |
| CVE | CVE-2024-56779 |
| CVE | CVE-2024-56780 |
| CVE | CVE-2024-56781 |
| CVE | CVE-2024-57802 |
| CVE | CVE-2024-57807 |
| CVE | CVE-2024-57849 |
| CVE | CVE-2024-57850 |
| CVE | CVE-2024-57884 |
| CVE | CVE-2024-57889 |
| CVE | CVE-2024-57890 |
| CVE | CVE-2024-57892 |
| CVE | CVE-2024-57900 |
| CVE | CVE-2024-57901 |
| CVE | CVE-2024-57902 |
| CVE | CVE-2024-57904 |
| CVE | CVE-2024-57906 |
| CVE | CVE-2024-57908 |
| CVE | CVE-2024-57910 |
| CVE | CVE-2024-57911 |
| CVE | CVE-2024-57912 |
| CVE | CVE-2024-57913 |
| CVE | CVE-2024-57922 |
| CVE | CVE-2024-57929 |
| CVE | CVE-2024-57931 |
| CVE | CVE-2024-57938 |
| CVE | CVE-2024-57946 |
| CVE | CVE-2024-57948 |
| CVE | CVE-2024-57951 |
| CVE | CVE-2025-21638 |
| CVE | CVE-2025-21639 |
| CVE | CVE-2025-21640 |
| CVE | CVE-2025-21653 |
| CVE | CVE-2025-21664 |
| CVE | CVE-2025-21678 |
| CVE | CVE-2025-21687 |
| CVE | CVE-2025-21689 |
| CVE | CVE-2025-21694 |
| CVE | CVE-2025-21697 |
| CVE | CVE-2025-21699 |
| XREF | USN:7391-1 |
| XREF | CISA-KNOWN-EXPLOITED:2025/04/30 |

Plugin Information

Published: 2025/04/01, Modified: 2025/04/09

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-211-generic for this advisory.

233783 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7408-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7408-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- SMB network file system;
- Network namespace;
- Networking core; (CVE-2024-56658, CVE-2024-35864, CVE-2024-26928)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7408-1>

Solution

Update the affected kernel package.

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-2024-26928 |
| CVE | CVE-2024-35864 |
| CVE | CVE-2024-56658 |
| XREF | USN:7408-1 |

Plugin Information

Published: 2025/04/02, Modified: 2025/04/02

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-212-generic for this advisory.

234814 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7461-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7461-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- GPU drivers;
- Network drivers;
- File systems infrastructure;

- Ext4 file system;
- Network file system (NFS) server daemon;
- Bluetooth subsystem;
- IPv6 networking;
- Network traffic control; (CVE-2024-53237, CVE-2024-50256, CVE-2021-47119, CVE-2024-35958, CVE-2025-21700, CVE-2025-21703, CVE-2024-56651, CVE-2024-49974, CVE-2025-21702, CVE-2024-26915, CVE-2024-46826)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7461-1>

Solution

Update the affected kernel package.

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-2021-47119 |
| CVE | CVE-2024-26915 |
| CVE | CVE-2024-35958 |
| CVE | CVE-2024-46826 |
| CVE | CVE-2024-49974 |
| CVE | CVE-2024-50256 |
| CVE | CVE-2024-53237 |
| CVE | CVE-2024-56651 |
| CVE | CVE-2025-21700 |
| CVE | CVE-2025-21702 |
| CVE | CVE-2025-21703 |
| XREF | USN:7461-1 |

Plugin Information

Published: 2025/04/24, Modified: 2025/04/24

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-214-generic for this advisory.

235357 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7495-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7495-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Network drivers;
- Ceph distributed file system;
- Netfilter; (CVE-2023-52927, CVE-2023-52664, CVE-2024-26689)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7495-1>

Solution

Update the affected kernel package.

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-2023-52664 |
| CVE | CVE-2023-52927 |
| CVE | CVE-2024-26689 |
| XREF | USN:7495-1 |

Plugin Information

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

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-215-generic for this advisory.

236878 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7516-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7516-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the

following subsystems:

- ARM64 architecture;
- PowerPC architecture;
- Block layer subsystem;
- Drivers core;
- Network block device driver;
- Character device driver;
- GPU drivers;
- HID subsystem;
- InfiniBand drivers;
- Media drivers;
- Network drivers;
- PPS (Pulse Per Second) driver;
- PTP clock framework;
- RapidIO drivers;
- Real Time Clock drivers;
- SCSI subsystem;
- SLIMbus drivers;
- QCOM SoC drivers;
- Trusted Execution Environment drivers;
- USB DSL drivers;
- USB Device Class drivers;
- USB core drivers;
- USB Gadget drivers;
- USB Host Controller drivers;
- Renesas USBHS Controller drivers;
- File systems infrastructure;
- BTRFS file system;
- NILFS2 file system;
- UBI file system;
- KVM subsystem;
- L3 Master device support module;
- Process Accounting mechanism;
- printk logging mechanism;
- Scheduler infrastructure;
- Tracing infrastructure;
- Memory management;

- 802.1Q VLAN protocol;
- B.A.T.M.A.N. meshing protocol;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Logical Link layer;
- NFC subsystem;
- Open vSwitch;
- Rose network layer;
- Network traffic control;
- Wireless networking;

- Tomoyo security module; (CVE-2025-21866, CVE-2025-21846, CVE-2025-21971, CVE-2025-21909, CVE-2024-58083, CVE-2025-21811, CVE-2025-21776, CVE-2024-58051, CVE-2025-21917, CVE-2025-21935, CVE-2025-21785, CVE-2021-47191, CVE-2025-21765, CVE-2025-21704, CVE-2025-21647, CVE-2024-58069, CVE-2025-21877, CVE-2025-21948, CVE-2024-58007, CVE-2024-58001, CVE-2025-21871, CVE-2024-58055, CVE-2025-21848, CVE-2025-21925, CVE-2024-58058, CVE-2025-21814, CVE-2025-21905, CVE-2025-21898, CVE-2025-21926, CVE-2025-21760, CVE-2024-57973, CVE-2025-21806, CVE-2024-58071, CVE-2025-21761, CVE-2025-21762, CVE-2024-57986, CVE-2025-21708, CVE-2025-21744, CVE-2024-26996, CVE-2024-50055, CVE-2024-58020, CVE-2025-21858, CVE-2025-21715, CVE-2025-21904, CVE-2025-21920, CVE-2024-56599, CVE-2025-21781, CVE-2025-21764, CVE-2025-21865, CVE-2025-21772, CVE-2024-58072, CVE-2025-21928, CVE-2025-21859, CVE-2025-21721, CVE-2025-21719, CVE-2025-21914, CVE-2025-21753, CVE-2024-58009, CVE-2024-57981, CVE-2024-58063, CVE-2024-58052, CVE-2025-21722, CVE-2024-57977, CVE-2025-21736, CVE-2025-21922, CVE-2024-26982, CVE-2025-21718, CVE-2025-21916, CVE-2025-21749, CVE-2025-21787, CVE-2024-58085, CVE-2024-58010, CVE-2024-57979, CVE-2024-57980, CVE-2025-21782, CVE-2025-21791, CVE-2025-21728, CVE-2023-52741, CVE-2025-21934, CVE-2024-58002, CVE-2025-21735, CVE-2025-21910, CVE-2025-21823, CVE-2024-58090, CVE-2025-21862, CVE-2025-21731, CVE-2025-21835, CVE-2024-58017, CVE-2024-58014, CVE-2025-21763)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7516-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|-----|----------------|
| CVE | CVE-2021-47191 |
| CVE | CVE-2023-52741 |
| CVE | CVE-2024-26982 |
| CVE | CVE-2024-26996 |
| CVE | CVE-2024-50055 |
| CVE | CVE-2024-56599 |
| CVE | CVE-2024-57973 |
| CVE | CVE-2024-57977 |

CVE-CVE-2024-57979
CVE-CVE-2024-57980
CVE-CVE-2024-57981
CVE-CVE-2024-57986
CVE-CVE-2024-58001
CVE-CVE-2024-58002
CVE-CVE-2024-58007
CVE-CVE-2024-58009
CVE-CVE-2024-58010
CVE-CVE-2024-58014
CVE-CVE-2024-58017
CVE-CVE-2024-58020
CVE-CVE-2024-58051
CVE-CVE-2024-58052
CVE-CVE-2024-58055
CVE-CVE-2024-58058
CVE-CVE-2024-58063
CVE-CVE-2024-58069
CVE-CVE-2024-58071
CVE-CVE-2024-58072
CVE-CVE-2024-58083
CVE-CVE-2024-58085
CVE-CVE-2024-58090
CVE-CVE-2025-21647
CVE-CVE-2025-21704
CVE-CVE-2025-21708
CVE-CVE-2025-21715
CVE-CVE-2025-21718
CVE-CVE-2025-21719
CVE-CVE-2025-21721
CVE-CVE-2025-21722
CVE-CVE-2025-21728
CVE-CVE-2025-21731
CVE-CVE-2025-21735
CVE-CVE-2025-21736
CVE-CVE-2025-21744
CVE-CVE-2025-21749
CVE-CVE-2025-21753
CVE-CVE-2025-21760
CVE-CVE-2025-21761
CVE-CVE-2025-21762
CVE-CVE-2025-21763
CVE-CVE-2025-21764
CVE-CVE-2025-21765
CVE-CVE-2025-21772
CVE-CVE-2025-21776
CVE-CVE-2025-21781
CVE-CVE-2025-21782
CVE-CVE-2025-21785
CVE-CVE-2025-21787
CVE-CVE-2025-21791
CVE-CVE-2025-21806
CVE-CVE-2025-21811
CVE-CVE-2025-21814
CVE-CVE-2025-21823
CVE-CVE-2025-21835
CVE-CVE-2025-21846
CVE-CVE-2025-21848
CVE-CVE-2025-21858
CVE-CVE-2025-21859
CVE-CVE-2025-21862
CVE-CVE-2025-21865
CVE-CVE-2025-21866
CVE-CVE-2025-21871
CVE-CVE-2025-21877
CVE-CVE-2025-21898
CVE-CVE-2025-21904
CVE-CVE-2025-21905
CVE-CVE-2025-21909
CVE-CVE-2025-21910
CVE-CVE-2025-21914
CVE-CVE-2025-21916
CVE-CVE-2025-21917
CVE-CVE-2025-21920
CVE-CVE-2025-21922
CVE-CVE-2025-21925
CVE-CVE-2025-21926
CVE-CVE-2025-21928
CVE-CVE-2025-21934
CVE-CVE-2025-21935
CVE-CVE-2025-21948
CVE-CVE-2025-21971

Plugin Information

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

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-216-generic for this advisory.

240211 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7585-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7585-1 advisory.

It was discovered that the CIFS network file system implementation in the Linux kernel did not properly verify the target namespace when handling upcalls. An attacker could use this to expose sensitive information. (CVE-2025-2312)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- PowerPC architecture;
- x86 architecture;
- iSCSI Boot Firmware Table Attributes driver;
- GPU drivers;
- HID subsystem;
- InfiniBand drivers;
- Media drivers;
- MemoryStick subsystem;
- Network drivers;
- NTB driver;
- PCI subsystem;
- SCSI subsystem;
- Thermal drivers;
- JFS file system;
- File systems infrastructure;
- Tracing infrastructure;
- 802.1Q VLAN protocol;
- Asynchronous Transfer Mode (ATM) subsystem;
- Bluetooth subsystem;
- IPv6 networking;
- Netfilter;
- Network traffic control;

- Sun RPC protocol;
- USB sound devices; (CVE-2025-22007, CVE-2025-21959, CVE-2025-22021, CVE-2025-22063, CVE-2025-22045, CVE-2024-58093, CVE-2022-49636, CVE-2025-22020, CVE-2024-53168, CVE-2025-22071, CVE-2025-39735, CVE-2025-21991, CVE-2025-21992, CVE-2025-21996, CVE-2025-22035, CVE-2023-53034, CVE-2025-22054, CVE-2025-23136, CVE-2025-22073, CVE-2024-56551, CVE-2025-22005, CVE-2025-37937, CVE-2021-47211, CVE-2025-22086, CVE-2025-21956, CVE-2025-38637, CVE-2025-22004, CVE-2025-22018, CVE-2025-22079, CVE-2025-21957, CVE-2025-21993)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7585-1>

Solution

Update the affected kernel package.

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-2021-47211 |
| CVE | CVE-2022-49636 |
| CVE | CVE-2023-53034 |
| CVE | CVE-2024-53168 |
| CVE | CVE-2024-56551 |
| CVE | CVE-2024-58093 |
| CVE | CVE-2025-2312 |
| CVE | CVE-2025-21956 |
| CVE | CVE-2025-21957 |
| CVE | CVE-2025-21959 |
| CVE | CVE-2025-21991 |
| CVE | CVE-2025-21992 |
| CVE | CVE-2025-21993 |
| CVE | CVE-2025-21996 |
| CVE | CVE-2025-22004 |
| CVE | CVE-2025-22005 |
| CVE | CVE-2025-22007 |
| CVE | CVE-2025-22018 |
| CVE | CVE-2025-22020 |
| CVE | CVE-2025-22021 |
| CVE | CVE-2025-22035 |
| CVE | CVE-2025-22045 |
| CVE | CVE-2025-22054 |
| CVE | CVE-2025-22063 |
| CVE | CVE-2025-22071 |
| CVE | CVE-2025-22073 |
| CVE | CVE-2025-22079 |
| CVE | CVE-2025-22086 |
| CVE | CVE-2025-23136 |
| CVE | CVE-2025-37937 |
| CVE | CVE-2025-38637 |
| CVE | CVE-2025-39735 |
| XREF | USN:7585-1 |

Plugin Information

Published: 2025/06/20, Modified: 2025/06/20

Plugin Output

file:///C:/Users/yashp/OneDrive/Desktop/Tiki VA Report Nessus.html

679/1068

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-218-generic for this advisory.

242901 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7671-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7671-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ACPI drivers;
- GPU drivers;
- SMB network file system;
- Memory management;
- Netfilter;
- Network traffic control; (CVE-2024-53051, CVE-2024-46787, CVE-2024-50047, CVE-2024-56662, CVE-2025-37890, CVE-2025-38001, CVE-2025-37997, CVE-2025-37932, CVE-2025-37798, CVE-2025-38177, CVE-2025-38000)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7671-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|-----|--------------------------------|
| CVE | CVE-2024-46787 |
| CVE | CVE-2024-50047 |
| CVE | CVE-2024-53051 |
| CVE | CVE-2024-56662 |
| CVE | CVE-2025-37798 |
| CVE | CVE-2025-37890 |
| CVE | CVE-2025-37932 |
| CVE | CVE-2025-37997 |
| CVE | CVE-2025-38000 |

CVE CVE-XREF
CVE-2025-38001
CVE-2025-38177
USN:7671-1

Plugin Information

Published: 2025/07/28, Modified: 2025/07/28

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-219-generic for this advisory.

141921 - Ubuntu 18.04 LTS / 20.04 LTS : MariaDB vulnerabilities (USN-4603-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4603-1 advisory.

It was discovered that MariaDB didn't properly validate the content of a packet received from a server. A remote attacker could use this vulnerability to sent a specially crafted file to cause a denial of service.

(CVE-2020-13249)

It was discovered that MariaDB has other security issues. An attacker can cause a hang or frequently repeatable crash (denial of service). (CVE-2020-15180, CVE-2020-2752, CVE-2020-2760, CVE-2020-2812, CVE-2020-2814)

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4603-1>

Solution

Update the affected 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

7.8 (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-XREF
CVE-2020-2752
CVE-2020-2760
CVE-2020-2812
CVE-2020-2814
CVE-2020-13249
CVE-2020-15180
XREF USN:4603-1

Plugin Information

Published: 2020/10/27, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.25-0ubuntu0.20.04.1

- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.25-0ubuntu0.20.04.1
```

149446 - Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4952-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4952-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.25 in Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.34.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-34.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-24.html>
<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-25.html> <https://www.oracle.com/security-alerts/cpuapr2021.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4952-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------------|
| CVE | CVE-2021-2146 |
| CVE | CVE-2021-2154 |
| CVE | CVE-2021-2162 |
| CVE | CVE-2021-2164 |
| CVE | CVE-2021-2166 |
| CVE | CVE-2021-2169 |
| CVE | CVE-2021-2170 |
| CVE | CVE-2021-2171 |
| CVE | CVE-2021-2172 |
| CVE | CVE-2021-2179 |
| CVE | CVE-2021-2180 |
| CVE | CVE-2021-2193 |
| CVE | CVE-2021-2194 |
| CVE | CVE-2021-2196 |
| CVE | CVE-2021-2201 |
| CVE | CVE-2021-2203 |
| CVE | CVE-2021-2208 |
| CVE | CVE-2021-2212 |
| CVE | CVE-2021-2215 |
| CVE | CVE-2021-2217 |
| CVE | CVE-2021-2226 |
| CVE | CVE-2021-2230 |
| CVE | CVE-2021-2232 |
| CVE | CVE-2021-2278 |
| CVE | CVE-2021-2293 |
| CVE | CVE-2021-2298 |
| CVE | CVE-2021-2299 |
| CVE | CVE-2021-2300 |
| CVE | CVE-2021-2301 |
| CVE | CVE-2021-2304 |
| CVE | CVE-2021-2305 |
| CVE | CVE-2021-2307 |
| CVE | CVE-2021-2308 |
| XREF | USN:4952-1 |
| XREF | CEA-ID:CEA-2021-0025 |

Plugin Information

Published: 2021/05/13, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.25-0ubuntu0.20.04.1
```

154414 - Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-5123-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5123-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.27 in Ubuntu 20.04 LTS, Ubuntu 21.04, and Ubuntu 21.10. Ubuntu 18.04 LTS has been updated to MySQL 5.7.36.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-36.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-27.html>
<https://www.oracle.com/security-alerts/cpuoct2021.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5123-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-2478 |
| CVE | CVE-2021-2479 |
| CVE | CVE-2021-2481 |
| CVE | CVE-2021-35546 |
| CVE | CVE-2021-35575 |
| CVE | CVE-2021-35577 |
| CVE | CVE-2021-35584 |
| CVE | CVE-2021-35591 |
| CVE | CVE-2021-35596 |
| CVE | CVE-2021-35597 |
| CVE | CVE-2021-35602 |
| CVE | CVE-2021-35604 |
| CVE | CVE-2021-35607 |
| CVE | CVE-2021-35608 |
| CVE | CVE-2021-35610 |
| CVE | CVE-2021-35612 |
| CVE | CVE-2021-35613 |
| CVE | CVE-2021-35622 |
| CVE | CVE-2021-35623 |
| CVE | CVE-2021-35624 |
| CVE | CVE-2021-35625 |
| CVE | CVE-2021-35626 |
| CVE | CVE-2021-35627 |
| CVE | CVE-2021-35628 |
| CVE | CVE-2021-35630 |
| CVE | CVE-2021-35631 |
| CVE | CVE-2021-35632 |
| CVE | CVE-2021-35633 |
| CVE | CVE-2021-35634 |
| CVE | CVE-2021-35635 |
| CVE | CVE-2021-35636 |
| CVE | CVE-2021-35637 |
| CVE | CVE-2021-35638 |
| CVE | CVE-2021-35639 |
| CVE | CVE-2021-35640 |
| CVE | CVE-2021-35641 |
| CVE | CVE-2021-35642 |
| CVE | CVE-2021-35643 |
| CVE | CVE-2021-35644 |
| CVE | CVE-2021-35645 |
| CVE | CVE-2021-35646 |
| CVE | CVE-2021-35647 |
| CVE | CVE-2021-35648 |
| XREF | USN:5123-1 |
| XREF | IAVA:2021-A-0487-S |

Plugin Information

Published: 2021/10/26, Modified: 2024/08/27

Plugin Output

file:///C:/Users/yashp/OneDrive/Desktop/Tiki VA Report Nessus.html

684/1068

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.27-0ubuntu0.20.04.1

157356 - Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-5270-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5270-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.28 in Ubuntu 20.04 LTS and Ubuntu 21.10. Ubuntu 18.04 LTS has been updated to MySQL 5.7.37.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-37.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-28.html>
<https://www.oracle.com/security-alerts/cpujan2022.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5270-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.2 (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)

STIG Severity

I

References

| | |
|-----|--------------------------------|
| CVE | CVE-2022-21245 |
| CVE | CVE-2022-21249 |
| CVE | CVE-2022-21253 |
| CVE | CVE-2022-21254 |
| CVE | CVE-2022-21256 |
| CVE | CVE-2022-21264 |
| CVE | CVE-2022-21265 |
| CVE | CVE-2022-21270 |
| CVE | CVE-2022-21301 |
| CVE | CVE-2022-21302 |
| CVE | CVE-2022-21303 |
| CVE | CVE-2022-21304 |

| | |
|------|--------------------|
| CVE | CVE-2022-21339 |
| CVE | CVE-2022-21342 |
| CVE | CVE-2022-21344 |
| CVE | CVE-2022-21348 |
| CVE | CVE-2022-21351 |
| CVE | CVE-2022-21358 |
| CVE | CVE-2022-21362 |
| CVE | CVE-2022-21367 |
| CVE | CVE-2022-21368 |
| CVE | CVE-2022-21370 |
| CVE | CVE-2022-21372 |
| CVE | CVE-2022-21374 |
| CVE | CVE-2022-21378 |
| CVE | CVE-2022-21379 |
| XREF | USN:5270-1 |
| XREF | IAVA:2022-A-0030-S |

Plugin Information

Published: 2022/02/03, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.28-0ubuntu0.20.04.3

161025 - Ubuntu 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-5410-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5410-1 advisory.

Lenny Wang discovered that NSS incorrectly handled certain messages. A remote attacker could possibly use this issue to cause servers compiled with NSS to stop responding, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5410-1>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools 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

6.5 (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)

References

| | |
|------|----------------|
| CVE | CVE-2020-25648 |
| XREF | USN:5410-1 |

Plugin Information

Published: 2022/05/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.49.1-1ubuntu1.7

149252 - Ubuntu 18.04 LTS / 20.04 LTS : OpenVPN vulnerabilities (USN-4933-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4933-1 advisory.

It was discovered that OpenVPN incorrectly handled certain data channel v2 packets. A remote attacker could possibly use this issue to inject packets using a victim's peer-id. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-11810)

It was discovered that OpenVPN incorrectly handled deferred authentication. When a server is configured to use deferred authentication, a remote attacker could possibly use this issue to bypass authentication and access control channel data. (CVE-2020-15078)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4933-1>

Solution

Update the affected openvpn package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-11810 |
| CVE | CVE-2020-15078 |
| XREF | USN:4933-1 |

Plugin Information

Published: 2021/05/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : openvpn_2.4.7-1ubuntu2
- Fixed package : openvpn_2.4.7-1ubuntu2.20.04.2

159331 - Ubuntu 18.04 LTS / 20.04 LTS : Paramiko vulnerability (USN-5351-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5351-1 advisory.

Jan Schejbal discovered that Paramiko incorrectly handled permissions when writing private key files. A local attacker could possibly use this issue to gain access to private keys.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5351-1>

Solution

Update the affected python-paramiko and / or python3-paramiko 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: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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-24302 |
| XREF | USN:5351-1 |

Plugin Information

Published: 2022/03/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-paramiko_2.6.0-2
- Fixed package : python3-paramiko_2.6.0-2ubuntu0.1

149818 - Ubuntu 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-4963-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4963-1 advisory.

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash or hang, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4963-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2021-25287 |
| CVE | CVE-2021-25288 |
| CVE | CVE-2021-28675 |
| CVE | CVE-2021-28676 |
| CVE | CVE-2021-28677 |
| CVE | CVE-2021-28678 |
| XREF | USN:4963-1 |

Plugin Information

Published: 2021/05/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.4

152145 - Ubuntu 18.04 LTS / 20.04 LTS : QPFD vulnerabilities (USN-5026-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5026-1 advisory.

It was discovered that QPFD incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPFD to consume resources, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-18020)

It was discovered that QPFD incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPFD to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2021-36978)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5026-1>

Solution

Update the affected 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-2018-18020 |
| CVE | CVE-2021-36978 |
| XREF | USN:5026-1 |

Plugin Information

Published: 2021/07/29, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libqpdf26_9.1.1-1build1
- Fixed package : libqpdf26_9.1.1-1ubuntu0.1

142464 - Ubuntu 18.04 LTS / 20.04 LTS : SPICE vdagent vulnerabilities (USN-4617-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4617-1 advisory.

Matthias Gerstner discovered that SPICE vdagent incorrectly handled the active_xfers hash table. A local attacker could possibly use this issue to cause SPICE vdagent to consume memory, resulting in a denial of service. (CVE-2020-25650)

Matthias Gerstner discovered that SPICE vdagent incorrectly handled the active_xfers hash table. A local attacker could possibly use this issue to cause SPICE vdagent to consume memory, resulting in a denial of service, or obtain sensitive file contents. (CVE-2020-25651)

Matthias Gerstner discovered that SPICE vdagent incorrectly handled a large number of client connections.

A local attacker could possibly use this issue to cause SPICE vdagent to consume resources, resulting in a denial of service. (CVE-2020-25652)

Matthias Gerstner discovered that SPICE vdagent incorrectly handled client connections. A local attacker could possibly use this issue to obtain sensitive information, paste clipboard contents, and transfer files into the active session. (CVE-2020-25653)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4617-1>

Solution

Update the affected spice-vdagent package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2020-25650 |
| CVE | CVE-2020-25651 |
| CVE | CVE-2020-25652 |
| CVE | CVE-2020-25653 |
| XREF | USN:4617-1 |

Plugin Information

Published: 2020/11/05, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : spice-vdagent_0.19.0-2
- Fixed package : spice-vdagent_0.19.0-2ubuntu0.2

160538 - Ubuntu 18.04 LTS / 20.04 LTS : SQLite vulnerability (USN-5403-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5403-1 advisory.

It was discovered that SQLite command-line component incorrectly handled certain queries. An attacker could possibly use this issue to cause a crash or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5403-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-36690 |
| XREF | USN:5403-1 |

Plugin Information

Published: 2022/05/05, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.31.1-4ubuntu0.2
- Fixed package : libsqlite3-0_3.31.1-4ubuntu0.3

152916 - Ubuntu 18.04 LTS / 20.04 LTS : Squashfs-Tools vulnerability (USN-5057-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5057-1 advisory.

Etienne Stalmans discovered that Squashfs-Tools mishandled certain malformed SQUASHFS files. An attacker could use this vulnerability to write arbitrary files to the filesystem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5057-1>

Solution

Update the affected squashfs-tools package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-40153 |
| XREF | USN:5057-1 |

Plugin Information

Published: 2021/08/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : squashfs-tools_1:4.4-1
- Fixed package : squashfs-tools_1:4.4-1ubuntu0.1

153391 - Ubuntu 18.04 LTS / 20.04 LTS : Squashfs-Tools vulnerability (USN-5078-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5078-1 advisory.

Richard Weinberger discovered that Squashfs-Tools mishandled certain malformed SQUASHFS files. An attacker could use this vulnerability to write arbitrary files to the filesystem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5078-1>

Solution

Update the affected squashfs-tools package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-41072 |
| XREF | USN:5078-1 |

Plugin Information

Published: 2021/09/15, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : squashfs-tools_1:4.4-1
- Fixed package : squashfs-tools_1:4.4-1ubuntu0.2
```

152953 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5058-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5058-1 advisory.

It was discovered that Thunderbird didn't ignore IMAP server responses prior to completion of the STARTTLS handshake. A person-in-the-middle could potentially exploit this to trick Thunderbird into showing incorrect information. (CVE-2021-29969)

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, or execute arbitrary code. (CVE-2021-29970, CVE-2021-29976, CVE-2021-29980, CVE-2021-29984, CVE-2021-29985, CVE-2021-29986, CVE-2021-29988, CVE-2021-29989, CVE-2021-30547)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5058-1>

Solution

Update the affected 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

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-2021-29969 |
| CVE | CVE-2021-29970 |
| CVE | CVE-2021-29976 |
| CVE | CVE-2021-29980 |
| CVE | CVE-2021-29984 |
| CVE | CVE-2021-29985 |
| CVE | CVE-2021-29986 |
| CVE | CVE-2021-29988 |
| CVE | CVE-2021-29989 |
| CVE | CVE-2021-30547 |
| XREF | USN:5058-1 |
| XREF | IAVA:2021-A-0309-S |
| XREF | IAVA:2021-A-0366-S |
| XREF | IAVA:2021-A-0293-S |

Plugin Information

Published: 2021/09/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:78.13.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:78.13.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:78.13.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:78.13.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:78.13.0+build1-0ubuntu0.20.04.2
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:78.13.0+build1-0ubuntu0.20.04.2

155308 - Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5146-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5146-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5146-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2021-38493 |
| XREF | USN:5146-1 |
| XREF | IAVA:2021-A-0405-S |

Plugin Information

Published: 2021/11/12, Modified: 2025/03/06

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:78.14.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:78.14.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:78.14.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:78.14.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:78.14.0+build1-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:78.14.0+build1-0ubuntu0.20.04.1

144789 - Ubuntu 18.04 LTS / 20.04 LTS : WavPack vulnerability (USN-4682-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4682-1 advisory.

It was discovered that WavPack incorrectly handled certain WAV files. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4682-1>

Solution

Update the affected libwavpack-dev, libwavpack1 and / or wavpack packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2020-35738
XREF-USN:4682-1

Plugin Information

Published: 2021/01/07, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libwavpack1_5.2.0-1
- Fixed package : libwavpack1_5.2.0-1ubuntu0.1

153568 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-5087-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5087-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5087-1>

Solution

Update the affected 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

8.2 (CVSS:3.0/E:F/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

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

STIG Severity

I

References

| | |
|------|---------------------------------|
| CVE | CVE-2021-30858 |
| XREF | USN:5087-1 |
| XREF | IAVA:2021-A-0414-S |
| XREF | CISA-KNOWN-EXPLOITED:2021/11/17 |

Plugin Information

Published: 2021/09/22, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.32.4-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.32.4-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.32.4-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.32.4-0ubuntu0.20.04.1

147979 - Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerability (USN-4739-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4739-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4739-1>

Solution

Update the affected 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

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-2020-13558 |
| XREF | USN:4739-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.30.5-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.30.5-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.30.5-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.30.5-0ubuntu0.20.04.1

152002 - Ubuntu 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-5021-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5021-1 advisory.

Harry Sintonen and Tomas Hoger discovered that curl incorrectly handled TELNET connections when the -t option was used on the command line. Uninitialized data possibly containing sensitive information could be sent to the remote server, contrary to expectations. (CVE-2021-22898, CVE-2021-22925)

Harry Sintonen discovered that curl incorrectly reused connections in the connection pool. This could result in curl reusing the wrong connections. (CVE-2021-22924)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5021-1>

Solution

Update the affected 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:L/I:N/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:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-22898 |
| CVE | CVE-2021-22924 |
| CVE | CVE-2021-22925 |
| XREF | USN:5021-1 |

Plugin Information

Published: 2021/07/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.6

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.6

153407 - Ubuntu 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-5079-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5079-1 advisory.

It was discovered that curl incorrectly handled memory when sending data to an MQTT server. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-22945)

Patrick Monnerat discovered that curl incorrectly handled upgrades to TLS. When receiving certain responses from servers, curl would continue without TLS even when the option to require a successful upgrade to TLS was specified. (CVE-2021-22946)

Patrick Monnerat discovered that curl incorrectly handled responses received before STARTTLS. A remote attacker could possibly use this issue to inject responses and intercept communications. (CVE-2021-22947)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5079-1>

Solution

Update the affected 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/V/A:H/SC:N/SI:N/SA:N)

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

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-2021-22945 |
| CVE | CVE-2021-22946 |
| CVE | CVE-2021-22947 |
| XREF | USN:5079-1 |

Plugin Information

Published: 2021/09/15, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.7
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.7

165321 - Ubuntu 18.04 LTS / 20.04 LTS : libjpeg-turbo vulnerabilities (USN-5631-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5631-1 advisory.

It was discovered that libjpeg-turbo incorrectly handled certain EOF characters. An attacker could possibly use this issue to cause libjpeg-turbo to consume resource, leading to a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-11813)

It was discovered that libjpeg-turbo incorrectly handled certain malformed jpeg files. An attacker could possibly use this issue to cause libjpeg-turbo to crash, resulting in a denial of service.
(CVE-2020-17541, CVE-2020-35538)

It was discovered that libjpeg-turbo incorrectly handled certain malformed PPM files. An attacker could use this issue to cause libjpeg-turbo to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-46822)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5631-1>

Solution

Update the affected 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

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-2018-11813 |
| CVE | CVE-2020-17541 |
| CVE | CVE-2020-35538 |
| CVE | CVE-2021-46822 |
| XREF | USN:5631-1 |

Plugin Information

Published: 2022/09/22, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libjpeg-turbo8_2.0.3-0ubuntu1.20.04.1
- Fixed package : libjpeg-turbo8_2.0.3-0ubuntu1.20.04.3

152136 - Ubuntu 18.04 LTS / 20.04 LTS : libsndfile vulnerability (USN-5025-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5025-1 advisory.

It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5025-1>

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs 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

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-2021-3246 |
| XREF | USN:5025-1 |

Plugin Information

Published: 2021/07/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsndfile1_1.0.28-7
- Fixed package : libsndfile1_1.0.28-7ubuntu0.1

159380 - Ubuntu 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5359-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5359-1 advisory.

Danilo Ramos discovered that rsync incorrectly handled memory when performing certain zlib deflating operations. An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5359-1>

Solution

Update the affected rsync package.

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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2018-25032 |
| XREF | USN:5359-1 |

Plugin Information

Published: 2022/03/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : rsync_3.1.3-8

- Fixed package : rsync_3.1.3-8ubuntu0.3

158135 - Ubuntu 18.04 LTS / 20.04 LTS : snapd vulnerabilities (USN-5292-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5292-1 advisory.

James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. (CVE-2021-3155)

Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. (CVE-2021-4120)

The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. (CVE-2021-44730)

The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code. (CVE-2021-44731)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5292-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

6.9 (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-2021-3155 |
| CVE | CVE-2021-4120 |
| CVE | CVE-2021-44730 |
| CVE | CVE-2021-44731 |
| XREF | USN:5292-1 |

Plugin Information

Published: 2022/02/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.54.3+20.04

151836 - Ubuntu 18.04 LTS / 20.04 LTS : systemd vulnerabilities (USN-5013-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5013-1 advisory.

It was discovered that systemd incorrectly handled certain mount paths. A local attacker could possibly use this issue to cause systemd to crash, resulting in denial of service. (CVE-2021-33910)

Mitchell Frank discovered that systemd incorrectly handled DHCP FORCERENEW packets. A remote attacker could possibly use this issue to reconfigure servers. (CVE-2020-13529)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5013-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.5 (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-2020-13529 |
| CVE | CVE-2021-33910 |
| XREF | USN:5013-1 |
| KREF | IAVA:2021-A-0350 |

Plugin Information

Published: 2021/07/20, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libnss-systemd_245.4-4ubuntu3.2
- Fixed package : libnss-systemd_245.4-4ubuntu3.10
- Installed package : libpam-systemd_245.4-4ubuntu3.2
- Fixed package : libpam-systemd_245.4-4ubuntu3.10
- Installed package : libsystemd0_245.4-4ubuntu3.2
- Fixed package : libsystemd0_245.4-4ubuntu3.10
- Installed package : libudev1_245.4-4ubuntu3.2
- Fixed package : libudev1_245.4-4ubuntu3.10
- Installed package : systemd_245.4-4ubuntu3.2
- Fixed package : systemd_245.4-4ubuntu3.10
- Installed package : systemd-sysv_245.4-4ubuntu3.2

- Fixed package : systemd-sysv_245.4-4ubuntu3.10
- Installed package : systemd-timesyncd_245.4-4ubuntu3.2
- Fixed package : systemd-timesyncd_245.4-4ubuntu3.10
- Installed package : udev_245.4-4ubuntu3.2
- Fixed package : udev_245.4-4ubuntu3.10

159631 - Ubuntu 18.04 LTS / 20.04 LTS : tcpdump vulnerabilities (USN-5331-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5331-2 advisory.

USN-5331-1 fixed several vulnerabilities in tcpdump. This update provides the corresponding update for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5331-2>

Solution

Update the affected tcpdump package.

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/V/A:H/SC:N/SI:N/SA:N)

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

6.8 (CVSS:3.0/E:U/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

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

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2018-16301 |
| CVE | CVE-2020-8037 |
| XREF | USN:5331-2 |
| XREF | IAVA:2021-A-0202-S |

Plugin Information

Published: 2022/04/11, Modified: 2024/10/30

Plugin Output

tcp/0

- Installed package : tcpdump_4.9.3-4
- Fixed package : tcpdump_4.9.3-4ubuntu0.1

159363 - Ubuntu 18.04 LTS / 20.04 LTS : zlib vulnerability (USN-5355-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5355-1 advisory.

Danilo Ramos discovered that zlib incorrectly handled memory when performing certain deflating operations.

An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5355-1>

Solution

Update the affected 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2018-25032 |
| XREF | USN:5355-1 |

Plugin Information

Published: 2022/03/31, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : zlib1g_1:1.2.11.dfsg-2ubuntu1
- Fixed package : zlib1g_1:1.2.11.dfsg-2ubuntu1.3

178481 - Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 : curl vulnerabilities (USN-6237-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6237-1 advisory.

- An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard patterns when listed as Subject Alternative Name in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one provided by a TLS library. This private wildcard matching

function would match IDN (International Domain Name) hosts incorrectly and could as a result accept patterns that otherwise should mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always start with 'xn--' and should not be allowed to pattern match, but the wildcard check in curl could still check for 'x*', which would match even though the IDN name most likely contained nothing even resembling an 'x'. (CVE-2023-28321)

- An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneously use the read callback ('CURLOPT_READFUNCTION') to ask for data to send, even when the 'CURLOPT_POSTFIELDS' option has been set, if the same handle previously was used to issue a 'PUT' request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST. (CVE-2023-28322)

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://ubuntu.com/security/notices/USN-6237-1>

Solution

Update the affected 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-2023-28322 |
| XREF | USN:6237-1 |
| XREF | IAVA:2023-A-0259-S |

Plugin Information

Published: 2023/07/19, Modified: 2023/08/31

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.19
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.19

186809 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNOME Settings vulnerability (USN-6554-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6554-1 advisory.

Zygmunt Krynicki discovered that GNOME Settings did not accurately reflect the SSH remote login status when the system was configured to use systemd socket activation for OpenSSH. Remote SSH access may be unknowingly enabled, contrary to expectation.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6554-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.3 (CVSS:3.0/E:U/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

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

References

| | |
|------|---------------|
| CVE | CVE-2023-5616 |
| XREF | USN:6554-1 |

Plugin Information

Published: 2023/12/13, Modified: 2025/04/16

Plugin Output

tcp/0

- Installed package : gnome-control-center_1:3.36.4-0ubuntu1
- Fixed package : gnome-control-center_1:3.36.5-0ubuntu4.1
- Installed package : gnome-control-center-data_1:3.36.4-0ubuntu1
- Fixed package : gnome-control-center-data_1:3.36.5-0ubuntu4.1
- Installed package : gnome-control-center-faces_1:3.36.4-0ubuntu1
- Fixed package : gnome-control-center-faces_1:3.36.5-0ubuntu4.1

186084 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerability (USN-6499-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6499-1 advisory.

It was discovered that GnuTLS had a timing side-channel when handling certain RSA-PSK key exchanges. A remote attacker could possibly use this issue to recover sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6499-1>

Solution

Update the affected 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/A: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 (CVSS:2.0/AV:N/AC:H/Au:N/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

4.0 (CVSS:2.0/E:U/RL:OF/RC:C)

References

CVE-2023-5981
XREF USN:6499-1

Plugin Information

Published: 2023/11/21, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.9

184027 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : MySQL vulnerabilities (USN-6459-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6459-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.35 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-35.html> <https://www.oracle.com/security-alerts/cpuoct2023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6459-1>

Solution

Update the affected 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-2023-22032 |
| CVE | CVE-2023-22059 |
| CVE | CVE-2023-22064 |
| CVE | CVE-2023-22066 |
| CVE | CVE-2023-22068 |
| CVE | CVE-2023-22070 |
| CVE | CVE-2023-22078 |
| CVE | CVE-2023-22079 |
| CVE | CVE-2023-22084 |
| CVE | CVE-2023-22092 |
| CVE | CVE-2023-22097 |
| CVE | CVE-2023-22103 |
| CVE | CVE-2023-22112 |
| CVE | CVE-2023-22114 |
| XREF | USN:6459-1 |

Plugin Information

Published: 2023/10/30, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.35-0ubuntu0.20.04.1

184088 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Open VM Tools vulnerabilities (USN-6463-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6463-1 advisory.

It was discovered that Open VM Tools incorrectly handled SAML tokens. A remote attacker Guest Operations privileges could possibly use this issue to escalate privileges. (CVE-2023-34058)

Matthias Gerstner discovered that Open VM Tools incorrectly handled file descriptors when dropping privileges. A local attacker could possibly use this issue to hijack /dev/uinput and simulate user inputs.

(CVE-2023-34059)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6463-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-34058 |
| CVE | CVE-2023-34059 |
| XREF | USN:6463-1 |

Plugin Information

Published: 2023/10/31, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : open-vm-tools_2:11.1.0-2ubuntu20.04.1
- Fixed package : open-vm-tools_2:11.3.0-2ubuntu0~ubuntu20.04.7
- Installed package : open-vm-tools-desktop_2:11.1.0-2ubuntu20.04.1
- Fixed package : open-vm-tools-desktop_2:11.3.0-2ubuntu0~ubuntu20.04.7

187627 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6565-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6565-1 advisory.

It was discovered that OpenSSH incorrectly handled supplemental groups when running helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand as a different user. An attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-41617)

It was discovered that OpenSSH incorrectly added destination constraints when PKCS#11 token keys were added to ssh-agent, contrary to expectations. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-51384)

It was discovered that OpenSSH incorrectly handled user names or host names with shell metacharacters. An attacker could possibly use this issue to perform OS command injection. (CVE-2023-51385)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6565-1>

Solution

Update the affected 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

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-2023-51384 |
| CVE | CVE-2023-51385 |
| XREF | IAVA:2021-A-0474-S |
| XREF | USN:6565-1 |
| XREF | IAVA:2023-A-0701-S |

Plugin Information

Published: 2024/01/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.11
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.11
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.11
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.11

189143 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : PAM vulnerability (USN-6588-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6588-1 advisory.

Matthias Gerstner discovered that the PAM pam_namespace module incorrectly handled special files when performing directory checks. A local attacker could possibly use this issue to cause PAM to stop responding, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6588-1>

Solution

Update the affected 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-2024-22365 |
| XREF | USN:6588-1 |

Plugin Information

Published: 2024/01/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libpam-modules_1.3.1-5ubuntu4
- Fixed package : libpam-modules_1.3.1-5ubuntu4.7
- Installed package : libpam-modules-bin_1.3.1-5ubuntu4
- Fixed package : libpam-modules-bin_1.3.1-5ubuntu4.7
- Installed package : libpam-runtime_1.3.1-5ubuntu4
- Fixed package : libpam-runtime_1.3.1-5ubuntu4.7
- Installed package : libpam0g_1.3.1-5ubuntu4
- Fixed package : libpam0g_1.3.1-5ubuntu4.7

183886 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6453-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6453-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled prepending values to certain properties. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-5367)

Sri discovered that the X.Org X Server incorrectly handled destroying windows in certain legacy multi- screen setups. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-5380)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6453-1>

Solution

Update the affected 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-2023-5367 |
| CVE | CVE-2023-5380 |
| XREF | USN:6453-1 |

Plugin Information

Published: 2023/10/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.9
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.9
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.9
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.9
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.9

186615 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : curl vulnerabilities (USN-6535-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6535-1 advisory.

Harry Sintonen discovered that curl incorrectly handled mixed case cookie domains. A remote attacker could possibly use this issue to set cookies that get sent to different and unrelated sites and domains.

(CVE-2023-46218)

Maksymilian Arciemowicz discovered that curl incorrectly handled long file names when saving HSTS data.

This could result in curl losing HSTS data, and subsequent requests to a site would be done without it, contrary to expectations. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-46219)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6535-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/NC:H/V:I:H/V:A: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-2023-46218 |
| CVE | CVE-2023-46219 |
| XREF | USN:6535-1 |
| XREF | IAVA:2023-A-0674-S |

Plugin Information

Published: 2023/12/06, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.21
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.21

189295 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerabilities (USN-6592-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6592-1 advisory.

It was discovered that libssh incorrectly handled the ProxyCommand and the ProxyJump features. A remote attacker could possibly use this issue to inject malicious code into the command of the features mentioned through the hostname parameter. (CVE-2023-6004)

It was discovered that libssh incorrectly handled return codes when performing message digest operations.

A remote attacker could possibly use this issue to cause libssh to crash, obtain sensitive information, or execute arbitrary code. (CVE-2023-6918)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6592-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2023-6004 |
| CVE | CVE-2023-6918 |
| XREF | USN:6592-1 |

Plugin Information

Published: 2024/01/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssh-4_0.9.3-2ubuntu2
- Fixed package : libssh-4_0.9.3-2ubuntu2.5

187106 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerability (USN-6561-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6561-1 advisory.

Fabian Bumer, Marcus Brinkmann, Jrg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6561-1>

Solution

Update the affected 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/V/A: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)

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2023-48795 |
| XREF | USN:6561-1 |
| XREF | IAVA:2023-A-0703 |

Plugin Information

Published: 2023/12/19, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : libssh-4_0.9.3-2ubuntu2
- Fixed package : libssh-4_0.9.3-2ubuntu2.4

186623 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : python-cryptography vulnerabilities (USN-6539-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6539-1 advisory.

It was discovered that the python-cryptography Cipher.update_into function would incorrectly accept objects with immutable buffers. This would result in corrupted output, contrary to expectations. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-23931)

It was discovered that python-cryptography incorrectly handled loading certain PKCS7 certificates. A remote attacker could possibly use this issue to cause python-cryptography to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-49083)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6539-1>

Solution

Update the affected python-cryptography and / or python3-cryptography 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/V/I:H/V/A: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:N/I:L/A:L)

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:N/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-23931 |
| CVE | CVE-2023-49083 |
| XREF | USN:6539-1 |

Plugin Information

Published: 2023/12/06, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : python3-cryptography_2.8-3
- Fixed package : python3-cryptography_2.8-3ubuntu0.2

177711 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : AccountsService vulnerability (USN-6190-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6190-1 advisory.

Kevin Backhouse discovered that AccountsService incorrectly handled certain D-Bus messages. A local attacker could use this issue to cause AccountsService to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6190-1>

Solution

Update the affected 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:I/C:A;C)

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2023-3297 |
| XREF | USN:6190-1 |

Plugin Information

Published: 2023/06/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : accountsservice_0.6.55-0ubuntu12~20.04.1
- Fixed package : accountsservice_0.6.55-0ubuntu12~20.04.6
- Installed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.1
- Fixed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.6
- Installed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.1
- Fixed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.6

176562 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Avahi vulnerability (USN-6129-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6129-1 advisory.

It was discovered that Avahi incorrectly handled certain DBus messages. A local attacker could possibly use this issue to cause Avahi to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6129-1>

Solution

Update the affected 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 (CVSS:2.0/AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.6 (CVSS:2.0/E:POC/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2023-1981 |
| XREF | USN:6129-1 |

Plugin Information

Published: 2023/06/01, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : avahi-autoipd_0.7-4ubuntu7
- Fixed package : avahi-autoipd_0.7-4ubuntu7.2

- Installed package : avahi-daemon_0.7-4ubuntu7
- Fixed package : avahi-daemon_0.7-4ubuntu7.2

- Installed package : avahi-utils_0.7-4ubuntu7
- Fixed package : avahi-utils_0.7-4ubuntu7.2

- Installed package : libavahi-client3_0.7-4ubuntu7
- Fixed package : libavahi-client3_0.7-4ubuntu7.2

- Installed package : libavahi-common-data_0.7-4ubuntu7
- Fixed package : libavahi-common-data_0.7-4ubuntu7.2

- Installed package : libavahi-common3_0.7-4ubuntu7
- Fixed package : libavahi-common3_0.7-4ubuntu7.2

- Installed package : libavahi-core7_0.7-4ubuntu7
- Fixed package : libavahi-core7_0.7-4ubuntu7.2

- Installed package : libavahi-glib1_0.7-4ubuntu7
- Fixed package : libavahi-glib1_0.7-4ubuntu7.2
```

- Installed package : libavahi-ui-gtk3-0_0.7-4ubuntu7
- Fixed package : libavahi-ui-gtk3-0_0.7-4ubuntu7.2

177536 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6184-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6184-1 advisory.

It was discovered that CUPS incorrectly handled certain memory operations. An attacker could possibly use this issue to cause CUPS to crash, resulting in a denial of service, or possibly obtain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6184-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-34241 |
| XREF | USN:6184-1 |

Plugin Information

Published: 2023/06/22, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.4
- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.4
- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.4
- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.4
- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.4
- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.4
- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.4

```
- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.4

- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.4

- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.4

- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.4
```

181317 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6361-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6361-1 advisory.

It was discovered that CUPS incorrectly authenticated certain remote requests. A remote attacker could possibly use this issue to obtain recently printed documents.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6361-1>

Solution

Update the affected 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2023-32360 |
| XREF | USN:6361-1 |

Plugin Information

Published: 2023/09/12, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.5

- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.5

- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.5

- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.5
```

```
- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.5

- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.5

- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.5

- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.5

- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.5

- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.5

- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.5
```

181687 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6391-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6391-1 advisory.

It was discovered that CUPS incorrectly parsed certain Postscript objects. If a user or automated system were tricked into printing a specially crafted document, a remote attacker could use this issue to cause CUPS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6391-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.0 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|-------------------------------|
| CVE | CVE-2023-4504 |
| XREF | USN:6391-1 |

Plugin Information

Published: 2023/09/20, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.6
```

```
- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.6

- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.6

- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.6

- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.6

- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.6

- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.6

- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.6

- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.6

- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.6

- Installed package : libcupsimage2_2.3.1-9ubuntu1.1
- Fixed package : libcupsimage2_2.3.1-9ubuntu1.6
```

175487 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : FreeType vulnerability (USN-6062-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6062-1 advisory.

It was discovered that FreeType incorrectly handled certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6062-1>

Solution

Update the affected packages.

Risk Factor

Medium

References

XREF USN:6062-1

Plugin Information

Published: 2023/05/13, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libfreetype6_2.10.1-2
- Fixed package : libfreetype6_2.10.1-2ubuntu0.3
```

184451 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Kerberos vulnerability (USN-6467-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6467-2 advisory.

USN-6467-1 fixed a vulnerability in Kerberos. This update provides the corresponding update for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.04.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6467-2>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/NC:H/VI:H/V/A: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 |
| XREF | USN:6467-2 |

Plugin Information

Published: 2023/11/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.4
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.4
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.4
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.4
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.4

[179881 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities \(USN-6288-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6288-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.34 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-34.html> <https://www.oracle.com/security-alerts/cpujul2023.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6288-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-22005 |
| CVE | CVE-2023-22008 |
| CVE | CVE-2023-22033 |
| CVE | CVE-2023-22038 |
| CVE | CVE-2023-22046 |
| CVE | CVE-2023-22048 |
| CVE | CVE-2023-22053 |
| CVE | CVE-2023-22054 |
| CVE | CVE-2023-22056 |
| CVE | CVE-2023-22057 |
| CVE | CVE-2023-22058 |
| XREF | USN:6288-1 |

Plugin Information

Published: 2023/08/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.34-0ubuntu0.20.04.1

181363 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6365-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6365-1 advisory.

It was discovered that Open VM Tools incorrectly handled SAML tokens. A remote attacker could possibly use this issue to bypass SAML token signature verification and perform VMware Tools Guest Operations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6365-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-20900
XREF USN:6365-1

Plugin Information

Published: 2023/09/13, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : open-vm-tools_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools_2:11.3.0-2ubuntu0~ubuntu20.04.6

- Installed package : open-vm-tools-desktop_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools-desktop_2:11.3.0-2ubuntu0~ubuntu20.04.6
```

186307 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6513-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6513-2 advisory.

USN-6513-1 fixed vulnerabilities in Python. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6513-2>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VCH:VI:H/V/A: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:L/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE
XREF
CVE-2023-40217
USN:6513-2

Plugin Information

Published: 2023/11/27, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.9

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.9

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.9

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.9

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.9
```

177111 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Requests vulnerability (USN-6155-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6155-1 advisory.

Dennis Brinkolf and Tobias Funke discovered that Requests incorrectly leaked Proxy-Authorization headers.
A remote attacker could possibly use this issue to obtain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6155-1>

Solution

Update the affected python3-requests package.

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/A: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-2023-32681
USN:6155-1

Plugin Information

Published: 2023/06/12, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : python3-requests_2.22.0-2ubuntu1
- Fixed package : python3-requests_2.22.0-2ubuntu1.1

178487 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Samba vulnerabilities (USN-6238-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6238-1 advisory.

It was discovered that Samba incorrectly handled Winbind NTLM authentication responses. An attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-2127)

Andreas Schneider discovered that Samba incorrectly enforced SMB2 packet signing. A remote attacker could possibly use this issue to obtain or modify sensitive information. This issue only affected Ubuntu 23.04.
(CVE-2023-3347)

Florent Saudel and Arnaud Gatignolof discovered that Samba incorrectly handled certain Spotlight requests.

A remote attacker could possibly use this issue to cause Samba to consume resources, leading to a denial of service. (CVE-2023-34966, CVE-2023-34967)

Ralph Boehme and Stefan Metzmacher discovered that Samba incorrectly handled paths returned by Spotlight requests. A remote attacker could possibly use this issue to obtain sensitive information.
(CVE-2023-34968)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6238-1>

Solution

Update the affected 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2022-2127 |
| CVE | CVE-2023-3347 |
| CVE | CVE-2023-34966 |
| CVE | CVE-2023-34967 |
| CVE | CVE-2023-34968 |
| XREF | USN:6238-1 |
| XREF | IAVA:2023-A-0376-S |

Plugin Information

Published: 2023/07/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `libsmbclient_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `libsmbclient_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `libwbclient0_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `libwbclient0_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `python3-samba_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `python3-samba_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba-common_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba-common_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba-common-bin_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba-dsdb-modules_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba-libs_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba-libs_2:4.15.13+dfsg-0ubuntu0.20.04.3`
- Installed package : `samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3`
- Fixed package : `samba-vfs-modules_2:4.15.13+dfsg-0ubuntu0.20.04.3`

[182845 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Samba vulnerabilities \(USN-6425-1\)](#)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6425-1 advisory.

Sri Nagasubramanian discovered that the Samba acl_xattr VFS module incorrectly handled read-only files.

When Samba is configured to ignore system ACLs, a remote attacker could possibly use this issue to truncate read-only files. (CVE-2023-4091)

Andrew Bartlett discovered that Samba incorrectly handled the DirSync control. A remote attacker with an RODC DC account could possibly use this issue to obtain all domain secrets. (CVE-2023-4154)

Andrew Bartlett discovered that Samba incorrectly handled the rpcecho development server. A remote attacker could possibly use this issue to cause Samba to stop responding, resulting in a denial of service. (CVE-2023-42669)

Kirin van der Veer discovered that Samba incorrectly handled certain RPC service listeners. A remote attacker could possibly use this issue to cause Samba to start multiple incompatible RPC listeners, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-42670)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6425-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2023-4091 |
| CVE | CVE-2023-4154 |
| CVE | CVE-2023-42669 |
| CVE | CVE-2023-42670 |
| XREF | USN:6425-1 |
| XREF | IAVA:2023-A-0535 |

Plugin Information

Published: 2023/10/10, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.15.13+dfsg-0ubuntu0.20.04.6

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.15.13+dfsg-0ubuntu0.20.04.6
```

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.15.13+dfsg-0ubuntu0.20.04.6
- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.15.13+dfsg-0ubuntu0.20.04.6

175285 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : WebKitGTK vulnerabilities (USN-6061-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6061-1 advisory.

Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6061-1>

Solution

Update the affected 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

8.2 (CVSS:3.0/E:F/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

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

References

| | |
|------|---------------------------------|
| CVE | CVE-2022-0108 |
| CVE | CVE-2023-25358 |
| CVE | CVE-2023-27932 |
| CVE | CVE-2023-27954 |
| CVE | CVE-2023-28205 |
| XREF | USN:6061-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/05/01 |

Plugin Information

Published: 2023/05/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.38.6-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.38.6-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.38.6-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.38.6-0ubuntu0.20.04.1

186986 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : YAJL vulnerabilities (USN-6233-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6233-2 advisory.

USN-6233-1 fixed vulnerabilities in YAJL. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6233-2>

Solution

Update the affected libyajl-dev, libyajl2 and / or yajl-tools 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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2017-16516 |
| CVE | CVE-2022-24795 |
| CVE | CVE-2023-33460 |
| XREF | USN:6233-2 |

Plugin Information

Published: 2023/12/15, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libyajl2_2.1.0-3
- Fixed package : libyajl2_2.1.0-3ubuntu0.20.04.1

182470 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libXpm vulnerabilities (USN-6408-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6408-1 advisory.

Yair Mizrahi discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to consume memory, leading to a denial of service. (CVE-2023-43786)

Yair Mizrahi discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could use this issue to cause libXpm to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-43787)

Alan Coopersmith discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to cause libXpm to crash, leading to a denial of service. (CVE-2023-43788, CVE-2023-43789)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6408-1>

Solution

Update the affected libxpm-dev, libxpm4 and / or xpmutils 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 |
| XREF | USN:6408-1 |

Plugin Information

Published: 2023/10/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libxpm4_1:3.5.12-1
- Fixed package : libxpm4_1:3.5.12-1ubuntu0.20.04.2

177325 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libcap2 vulnerabilities (USN-6166-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6166-1 advisory.

David Gstir discovered that libcap2 incorrectly handled certain return codes. An attacker could possibly use this issue to cause libcap2 to consume memory, leading to a denial of service. (CVE-2023-2602)

Richard Weinberger discovered that libcap2 incorrectly handled certain long input strings. An attacker could use this issue to cause libcap2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-2603)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6166-1>

Solution

Update the affected 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

7.8 (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-2023-2602 |
| CVE | CVE-2023-2603 |
| XREF | USN:6166-1 |

Plugin Information

Published: 2023/06/14, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : libcap2_1:2.32-1
- Fixed package : libcap2_1:2.32-1ubuntu0.1
- Installed package : libcap2-bin_1:2.32-1
- Fixed package : libcap2-bin_1:2.32-1ubuntu0.1
- Installed package : libpam-cap_1:2.32-1
- Fixed package : libpam-cap_1:2.32-1ubuntu0.1

179146 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : librsvg vulnerability (USN-6266-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6266-1 advisory.

Zac Sims discovered that librsvg incorrectly handled decoding URLs. A remote attacker could possibly use this issue to read arbitrary files by using an include element.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6266-1>

Solution

Update the affected 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: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-38633 |
| XREF | USN:6266-1 |

Plugin Information

Published: 2023/08/01, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-rsvg-2.0_2.48.7-1ubuntu0.20.04.1
- Fixed package : gir1.2-rsvg-2.0_2.48.9-1ubuntu0.20.04.4
- Installed package : librsvg2-2_2.48.7-1ubuntu0.20.04.1
- Fixed package : librsvg2-2_2.48.9-1ubuntu0.20.04.4
- Installed package : librsvg2-common_2.48.7-1ubuntu0.20.04.1
- Fixed package : librsvg2-common_2.48.9-1ubuntu0.20.04.4

176712 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libssh vulnerabilities (USN-6138-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6138-1 advisory.

Philip Turnbull discovered that libssh incorrectly handled rekeying with algorithm guessing. A remote attacker could use this issue to cause libssh to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-1667)

Kevin Backhouse discovered that libssh incorrectly handled verifying data signatures. A remote attacker could possibly use this issue to bypass authorization. (CVE-2023-2283)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6138-1>

Solution

Update the affected 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: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

II

References

| | |
|------|--------------------|
| CVE | CVE-2023-1667 |
| CVE | CVE-2023-2283 |
| XREF | USN:6138-1 |
| XREF | IAVA:2023-A-0517-S |

Plugin Information

Published: 2023/06/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssh-4_0.9.3-2ubuntu2
- Fixed package : libssh-4_0.9.3-2ubuntu2.3

182471 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libx11 vulnerabilities (USN-6407-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6407-1 advisory.

Gregory James Duck discovered that libx11 incorrectly handled certain keyboard symbols. If a user were tricked into connecting to a malicious X server, a remote attacker could use this issue to cause libx11 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-43785)

Yair Mizrahi discovered that libx11 incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to consume memory, leading to a denial of service. (CVE-2023-43786)

Yair Mizrahi discovered that libx11 incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could use this issue to cause libx11 to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-43787)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6407-1>

Solution

Update the affected 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 |
| XREF | USN:6407-1 |

Plugin Information

Published: 2023/10/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libx11-6_2:1.6.9-2ubuntu1
- Fixed package : libx11-6_2:1.6.9-2ubuntu1.6
- Installed package : libx11-data_2:1.6.9-2ubuntu1
- Fixed package : libx11-data_2:1.6.9-2ubuntu1.6
- Installed package : libx11-xcb1_2:1.6.9-2ubuntu1
- Fixed package : libx11-xcb1_2:1.6.9-2ubuntu1.6

179334 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : poppler vulnerabilities (USN-6273-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6273-1 advisory.

Jieyong Ma discovered that poppler incorrectly handled certain malformed PDF files. A remote attacker could possibly use this issue to cause poppler to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-27337)

It was discovered that poppler incorrectly handled certain malformed PDF files. A remote attacker could possibly use this issue to cause poppler to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-34872)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6273-1>

Solution

Update the affected 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

5.9 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2022-27337 |
| CVE | CVE-2023-34872 |
| XREF | USN:6273-1 |
| XREF | IAVB:2023-B-0075-S |

Plugin Information

Published: 2023/08/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.2
- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.2
- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.2
- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.2

200259 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : MySQL vulnerabilities (USN-6823-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6823-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.37 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.10, and Ubuntu 24.04 LTS.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-37.html> <https://www.oracle.com/security-alerts/cpuapr2024.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6823-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

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-2024-20994 |
| CVE | CVE-2024-20998 |
| CVE | CVE-2024-21000 |
| CVE | CVE-2024-21008 |
| CVE | CVE-2024-21009 |
| CVE | CVE-2024-21013 |
| CVE | CVE-2024-21047 |
| CVE | CVE-2024-21054 |
| CVE | CVE-2024-21060 |
| CVE | CVE-2024-21062 |
| CVE | CVE-2024-21069 |
| CVE | CVE-2024-21087 |
| CVE | CVE-2024-21096 |
| CVE | CVE-2024-21102 |
| XREF | USN:6823-1 |

Plugin Information

Published: 2024/06/10, Modified: 2025/04/10

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.37-0ubuntu0.20.04.3

201048 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Netplan vulnerabilities (USN-6851-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6851-1 advisory.

Andreas Hasenack discovered that netplan incorrectly handled the permissions for netdev files containing wireguard configuration. An attacker could use this to obtain wireguard secret keys.

It was discovered that netplan configuration could be manipulated into injecting arbitrary commands while setting up network interfaces. An attacker could use this to execute arbitrary commands or escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6851-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S: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

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2022-4968 |
| XREF | USN:6851-1 |

Plugin Information

Published: 2024/06/26, Modified: 2024/10/31

Plugin Output

tcp/0

- Installed package : libnetplan0_0.99-0ubuntu3~20.04.2
- Fixed package : libnetplan0_0.104-0ubuntu2~20.04.5
- Installed package : netplan.io_0.99-0ubuntu3~20.04.2
- Fixed package : netplan.io_0.104-0ubuntu2~20.04.5

201237 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : OpenVPN vulnerabilities (USN-6860-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6860-1 advisory.

Reynir Bjrnsson discovered that OpenVPN incorrectly handled terminating client connections. A remote authenticated client could possibly use this issue to keep the connection active, bypassing certain security policies. This issue only affected Ubuntu 23.10, and Ubuntu 24.04 LTS. (CVE-2024-28882)

Reynir Bjrnsson discovered that OpenVPN incorrectly handled certain control channel messages with nonprintable characters. A remote attacker could possibly use this issue to cause OpenVPN to consume resources, or fill up log files with garbage, leading to a denial of service. (CVE-2024-5594)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6860-1>

Solution

Update the affected openvpn package.

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

7.9 (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:N/A:P)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-5594 |
| CVE | CVE-2024-28882 |
| XREF | USN:6860-1 |
| XREF | IAVA:2024-A-0608-S |

Plugin Information

Published: 2024/07/02, Modified: 2025/04/03

Plugin Output

tcp/0

- Installed package : openvpn_2.4.7-1ubuntu2
- Fixed package : openvpn_2.4.12-0ubuntu0.20.04.2

198063 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6796-1 advisory.

Fergus Dall discovered that TPM2 Software Stack did not properly handle layer arrays. An attacker could possibly use this issue to cause

TPM2 Software Stack to crash, resulting in a denial of service, or

possibly execute arbitrary code. (CVE-2023-22745)

Jurgen Repp and Andreas Fuchs discovered that TPM2 Software Stack did not

validate the quote data after deserialization. An attacker could generate an arbitrary quote and cause TPM2 Software Stack to have unknown behavior.

(CVE-2024-29040)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6796-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2023-22745 |
| CVE | CVE-2024-29040 |
| XREF | USN:6796-1 |

Plugin Information

Published: 2024/05/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtss2-esys0_2.3.2-1
- Fixed package : libtss2-esys0_2.3.2-1ubuntu0.20.04.2

194475 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6755-1 advisory.

Ingo Brckl discovered that cpio contained a path traversal vulnerability. If a user or automated system were tricked into extracting a specially crafted cpio archive, an attacker could possibly use this issue to write arbitrary files outside the target directory on the host, even if using the option --no-absolute-filenames.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6755-1>

Solution

Update the affected cpio and / or cpio-win32 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:H/I:N/A:N)

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2023-7207 |
| XREF | USN:6755-1 |

Plugin Information

Published: 2024/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : cpio_2.13+dfsg-2
- Fixed package : cpio_2.13+dfsg-2ubuntu0.4

193341 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6733-1 advisory.

It was discovered that GnuTLS had a timing side-channel when performing certain ECDSA operations. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2024-28834)

It was discovered that GnuTLS incorrectly handled verifying certain PEM bundles. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2024-28835)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6733-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-28834 |
| CVE | CVE-2024-28835 |
| XREF | USN:6733-1 |

Plugin Information

Published: 2024/04/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.11

189536 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MariaDB vulnerabilities (USN-6600-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6600-1 advisory.

Several security issues were discovered in MariaDB and this update includes new upstream MariaDB versions to fix these issues.

MariaDB has been updated to 10.3.39 in Ubuntu 20.04 LTS, 10.6.16 in Ubuntu 22.04 LTS and 10.11.6 in Ubuntu 23.10.

CVE-2022-47015 only affected the MariaDB packages in Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6600-1>

Solution

Update the affected 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 |
| CVE | CVE-2023-22084 |
| XREF | USN:6600-1 |

Plugin Information

Published: 2024/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.39-0ubuntu0.20.04.2

- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.39-0ubuntu0.20.04.2
```

189776 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MySQL vulnerabilities (USN-6615-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6615-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.36 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-36.html> <https://www.oracle.com/security-alerts/cpujan2024.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6615-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2024-20960 |
| CVE | CVE-2024-20961 |
| CVE | CVE-2024-20962 |
| CVE | CVE-2024-20963 |
| CVE | CVE-2024-20964 |
| CVE | CVE-2024-20965 |
| CVE | CVE-2024-20966 |
| CVE | CVE-2024-20967 |
| CVE | CVE-2024-20969 |
| CVE | CVE-2024-20970 |
| CVE | CVE-2024-20971 |
| CVE | CVE-2024-20972 |
| CVE | CVE-2024-20973 |
| CVE | CVE-2024-20974 |
| CVE | CVE-2024-20976 |
| CVE | CVE-2024-20977 |
| CVE | CVE-2024-20978 |
| CVE | CVE-2024-20981 |
| CVE | CVE-2024-20982 |
| CVE | CVE-2024-20983 |
| CVE | CVE-2024-20984 |
| CVE | CVE-2024-20985 |
| XREF | USN:6615-1 |

Plugin Information

Published: 2024/01/30, Modified: 2025/06/04

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.36-0ubuntu0.20.04.1

193171 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6727-1 advisory.

It was discovered that NSS incorrectly handled padding when checking PKCS#1 certificates. A remote attacker could possibly use this issue to perform Bleichenbacher-like attacks and recover private data.

This issue only affected Ubuntu 20.04 LTS. (CVE-2023-4421)

It was discovered that NSS had a timing side-channel when performing RSA decryption. A remote attacker could possibly use this issue to recover private data. (CVE-2023-5388)

It was discovered that NSS had a timing side-channel when using certain NIST curves. A remote attacker could possibly use this issue to recover private data. (CVE-2023-6135)

The NSS package contained outdated CA certificates. This update refreshes the NSS package to version 3.98 which includes the latest CA certificate bundle and other security improvements.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6727-1>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|---------------|
| CVE | CVE-2023-4421 |
| CVE | CVE-2023-5388 |
| CVE | CVE-2023-6135 |
| XREF | USN:6727-1 |

Plugin Information

Published: 2024/04/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.98-0ubuntu0.20.04.1

189519 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Paramiko vulnerability (USN-6598-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6598-1 advisory.

Fabian Bumer, Marcus Brinkmann, Jrg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6598-1>

Solution

Update the affected python3-paramiko package.

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/Vl: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 |
| XREF | USN:6598-1 |

Plugin Information

Published: 2024/01/25, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : python3-paramiko_2.6.0-2
- Fixed package : python3-paramiko_2.6.0-2ubuntu0.3

200724 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6840-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6840-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code.(CVE-

2024-5688, CVE-2024-5690, CVE-2024-5696, CVE-2024-5700, CVE-2024-5702)

Luan Herrera discovered that Thunderbird did not properly validate the X-Frame-Options header inside sandboxed iframe. An attacker could potentially exploit this issue to bypass sandbox restrictions to open a new window. (CVE-2024-5691)

Kirtikumar Anandrao Ramchandani discovered that Thunderbird did not properly track cross-origin tainting in Offscreen Canvas. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2024-5693)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6840-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.2 (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-2024-5688 |
| CVE | CVE-2024-5690 |
| CVE | CVE-2024-5691 |
| CVE | CVE-2024-5693 |
| CVE | CVE-2024-5696 |
| CVE | CVE-2024-5700 |
| CVE | CVE-2024-5702 |
| XREF | USN:6840-1 |
| XREF | IAVA:2024-A-0387-S |

Plugin Information

Published: 2024/06/19, Modified: 2025/04/07

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.12.0+build3-0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.12.0+build3-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.12.0+build3-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.12.0+build3-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.12.0+build3-0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.12.0+build3-0ubuntu0.20.04.1

192629 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-1 advisory.

Skyler Ferrante discovered that the util-linux wall command did not filter escape sequences from command line arguments. A local attacker could possibly use this issue to obtain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6719-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

6.2 (CVSS:2.0/AV:L/AC:L/Au:S/C:I/I:A:N)

CVSS v2.0 Temporal Score

4.9 (CVSS:2.0/E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-28085 |
| XREF | USN:6719-1 |

Plugin Information

Published: 2024/03/27, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : bsutils_1:2.34-0.1ubuntu9
- Fixed package : bsutils_1:2.34-0.1ubuntu9.5

- Installed package : fdisk_2.34-0.1ubuntu9
- Fixed package : fdisk_2.34-0.1ubuntu9.5

- Installed package : libblkid1_2.34-0.1ubuntu9
- Fixed package : libblkid1_2.34-0.1ubuntu9.5

- Installed package : libfdisk1_2.34-0.1ubuntu9
- Fixed package : libfdisk1_2.34-0.1ubuntu9.5

- Installed package : libmount1_2.34-0.1ubuntu9
- Fixed package : libmount1_2.34-0.1ubuntu9.5

- Installed package : libsmartcols1_2.34-0.1ubuntu9
- Fixed package : libsmartcols1_2.34-0.1ubuntu9.5

- Installed package : libuuid1_2.34-0.1ubuntu9
- Fixed package : libuuid1_2.34-0.1ubuntu9.5

- Installed package : mount_2.34-0.1ubuntu9
- Fixed package : mount_2.34-0.1ubuntu9.5
```

- Installed package : rfkill_2.34-0.1ubuntu9
- Fixed package : rfkill_2.34-0.1ubuntu9.5
- Installed package : util-linux_2.34-0.1ubuntu9
- Fixed package : util-linux_2.34-0.1ubuntu9.5
- Installed package : uuid-runtime_2.34-0.1ubuntu9
- Fixed package : uuid-runtime_2.34-0.1ubuntu9.5

193159 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-2 advisory.

USN-6719-1 fixed a vulnerability in util-linux. Unfortunately, it was discovered that the fix did not fully address the issue. This update removes the setgid permission bit from the wall and write utilities.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6719-2>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-28085 |
| XREF | USN:6719-2 |

Plugin Information

Published: 2024/04/10, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : bsutils_1:2.34-0.1ubuntu9
- Fixed package : bsutils_1:2.34-0.1ubuntu9.6
- Installed package : fdisk_2.34-0.1ubuntu9
- Fixed package : fdisk_2.34-0.1ubuntu9.6
- Installed package : libblkid1_2.34-0.1ubuntu9
- Fixed package : libblkid1_2.34-0.1ubuntu9.6
- Installed package : libfdisk1_2.34-0.1ubuntu9
- Fixed package : libfdisk1_2.34-0.1ubuntu9.6

- Installed package : libmount1_2.34-0.1ubuntu9
- Fixed package : libmount1_2.34-0.1ubuntu9.6
- Installed package : libsmartcols1_2.34-0.1ubuntu9
- Fixed package : libsmartcols1_2.34-0.1ubuntu9.6
- Installed package : libuuid1_2.34-0.1ubuntu9
- Fixed package : libuuid1_2.34-0.1ubuntu9.6
- Installed package : mount_2.34-0.1ubuntu9
- Fixed package : mount_2.34-0.1ubuntu9.6
- Installed package : rfkill_2.34-0.1ubuntu9
- Fixed package : rfkill_2.34-0.1ubuntu9.6
- Installed package : util-linux_2.34-0.1ubuntu9
- Fixed package : util-linux_2.34-0.1ubuntu9.6
- Installed package : uuid-runtime_2.34-0.1ubuntu9
- Fixed package : uuid-runtime_2.34-0.1ubuntu9.6

237250 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : GLib vulnerability (USN-7532-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7532-1 advisory.

It was discovered that Glib incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7532-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-4373 |
| XREF | USN:7532-1 |
| XREF | IAVA:2025-A-0464 |

Plugin Information

Published: 2025/05/26, Modified: 2025/07/04

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.9
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.9
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.9

235829 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Open VM Tools vulnerability (USN-7508-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7508-1 advisory.

It was discovered that Open VM Tools incorrectly handled certain file operations. An attacker in a guest could use this issue to perform insecure file operations and possibly elevate privileges in the guest.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7508-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|------|----------------|
| CVE | CVE-2025-22247 |
| XREF | USN:7508-1 |

Plugin Information

Published: 2025/05/13, Modified: 2025/05/13

Plugin Output

tcp/0

- Installed package : open-vm-tools_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools_2:11.3.0-2ubuntu0~ubuntu20.04.8
- Installed package : open-vm-tools-desktop_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools-desktop_2:11.3.0-2ubuntu0~ubuntu20.04.8

237384 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : net-tools vulnerability (USN-7537-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has a package installed that is affected by a vulnerability as referenced in the USN-7537-1 advisory.

It was discovered that net-tools incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7537-1>

Solution

Update the affected net-tools package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2025-46836 |
| XREF | USN:7537-1 |

Plugin Information

Published: 2025/05/27, Modified: 2025/05/27

Plugin Output

tcp/0

- Installed package : net-tools_1.60+git20180626.aebd88e-1ubuntu1
- Fixed package : net-tools_1.60+git20180626.aebd88e-1ubuntu1.1

216857 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU binutils vulnerabilities (USN-7306-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7306-1 advisory.

It was discovered that GNU binutils in nm tool is affected by an incorrect access control. An attacker could possibly use this issue to cause a crash. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2024-57360)

It was discovered that GNU binutils incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2025-0840)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7306-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

6.3 (CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2024-57360 |
| CVE | CVE-2025-0840 |
| XREF | IAVA:2025-A-0095 |
| XREF | USN:7306-1 |

Plugin Information

Published: 2025/02/26, Modified: 2025/03/04

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.10
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.10
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.10
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.10
- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.10
- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.10

233981 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU binutils vulnerabilities (USN-7423-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7423-1 advisory.

It was discovered that GNU binutils incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash, expose sensitive information or execute arbitrary code. (CVE-2025-1153, CVE-2025-1182)

It was discovered that ld in GNU binutils incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2025-1176)

It was discovered that ld in GNU binutils incorrectly handled certain files. An attacker could possibly use this issue to cause a crash, expose sensitive information or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2025-1178, CVE-2025-1181)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7423-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

6.3 (CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/V:I:L/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

5.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

4.5 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-1153 |
| CVE | CVE-2025-1176 |
| CVE | CVE-2025-1178 |
| CVE | CVE-2025-1181 |
| CVE | CVE-2025-1182 |
| XREF | IAVA:2025-A-0095 |
| XREF | USN:7423-1 |

Plugin Information

Published: 2025/04/08, Modified: 2025/04/08

Plugin Output

tcp/0

- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.11
- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.11
- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.11
- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.11

- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.11

- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.11

233470 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Ghostscript vulnerabilities (USN-7378-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7378-1 advisory.

It was discovered that Ghostscript incorrectly serialized DollarBlend in certain fonts. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-27830)

It was discovered that Ghostscript incorrectly handled the DOCXWRITE TXTWRITE device. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2025-27831)

It was discovered that Ghostscript incorrectly handled the NPDL device. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2025-27832)

It was discovered that Ghostscript incorrectly handled certain long TTF file names. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 24.04 LTS and Ubuntu 24.10. (CVE-2025-27833)

It was discovered that Ghostscript incorrectly handled oversized Type 4 functions in certain PDF documents. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. (CVE-2025-27834)

It was discovered that Ghostscript incorrectly handled converting certain glyphs to Unicode. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-27835)

It was discovered that Ghostscript incorrectly handled the BJ10V device. An attacker could use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2025-27836)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7378-1>

Solution

Update the affected 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

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-27830 |
| CVE | CVE-2025-27831 |
| CVE | CVE-2025-27832 |
| CVE | CVE-2025-27833 |
| CVE | CVE-2025-27834 |
| CVE | CVE-2025-27835 |
| CVE | CVE-2025-27836 |
| XREF | IAVB:2025-B-0043 |
| XREF | USN:7378-1 |

Plugin Information

Published: 2025/03/28, Modified: 2025/03/28

Plugin Output

tcp/0

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.15
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.15
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.15
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.15

216587 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GnuTLS vulnerability (USN-7281-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7281-1 advisory.

Bing Shi discovered that GnuTLS incorrectly handled decoding certain DER-encoded certificates. A remote attacker could possibly use this issue to cause GnuTLS to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7281-1>

Solution

Update the affected 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: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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-12243 |
| XREF | USN:7281-1 |

Plugin Information

Published: 2025/02/21, Modified: 2025/02/21

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.12

217107 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerabilities (USN-7314-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7314-1 advisory.

It was discovered that Kerberos incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause Kerberos to consume memory, leading to a denial of service.
(CVE-2024-26458, CVE-2024-26461)

It was discovered that Kerberos incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause Kerberos to consume memory, leading to a denial of service. This issue only affected Ubuntu 24.04 LTS. (CVE-2024-26462)

It was discovered that the Kerberos kadm5 daemon incorrectly handled log files when incremental propagation was enabled. An authenticated attacker could use this issue to cause kadm5 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-24528)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7314-1>

Solution

Update the affected 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-2024-26458 |
| CVE | CVE-2024-26461 |
| CVE | CVE-2024-26462 |
| CVE | CVE-2025-24528 |
| XREF | USN:7314-1 |

Plugin Information

Published: 2025/03/03, Modified: 2025/03/04

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.9
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.9
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.9
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.9
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.9

214671 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerabilities (USN-7228-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7228-1 advisory.

Thomas Rinsma discovered that LibreOffice incorrectly handled paths when processing embedded font files.

If a user or automated system were tricked into opening a specially crafted LibreOffice file, a remote attacker could possibly use this issue to create arbitrary files ending with .ttf. (CVE-2024-12425)

Thomas Rinsma discovered that LibreOffice incorrectly handled certain environment variables and INI file values. If a user or automated system were tricked into opening a specially crafted LibreOffice file, a remote attacker could possibly use this issue to exfiltrate sensitive information. (CVE-2024-12426)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7228-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

6.7 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/V/C:H/V/I:N/V/A:N/SC:H/S/I: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

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C: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-2024-12425 |
| CVE | CVE-2024-12426 |
| XREF | USN:7228-1 |
| XREF | IAVB:2025-B-0003-S |

Plugin Information

Published: 2025/01/27, Modified: 2025/03/06

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.13
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-l10n-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_gb_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.13

- Installed package : libridl-jar_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-jar_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.13
- Installed package : libunoloader-jar_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-jar_1:6.4.7-0ubuntu0.20.04.13
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.13
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.13
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.13

232550 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerability (USN-7337-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7337-1 advisory.

It was discovered that LibreOffice incorrectly handled Office URI Schemes. If a user or automated system were tricked into opening a specially crafted LibreOffice file, a remote attacker could possibly use this issue to call internal macros.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7337-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

7.2 (CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/Vl:L/VA:H/SC:H/SI:H/SA:H)

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

7.9 (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

|

References

| | |
|------|--------------------|
| CVE | CVE-2025-1080 |
| XREF | USN:7337-1 |
| XREF | IAVB:2025-B-0036-S |

Plugin Information

Published: 2025/03/10, Modified: 2025/05/05

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.14
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.14

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libuno-purpenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purpenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.14
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.14
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.14
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.14
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.14

235613 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerability (USN-7504-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7504-1 advisory.

Juraj arinay discovered that LibreOffice incorrectly handled verifying PDF signatures. A remote attacker could possibly use this issue to generate PDF files that appear to have a valid signature.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7504-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

2.4 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:L/VI:N/V/A:N/SC:L/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: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:O/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-2866 |
| XREF | IAVB:2025-B-0063 |
| XREF | USN:7504-1 |

Plugin Information

Published: 2025/05/08, Modified: 2025/05/08

Plugin Output

tcp/0

```
- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.15

- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-help-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_gb_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-help-en_us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en_us_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-l10n-en_gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_gb_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-l10n-en_za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en_za_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.15

- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.15
```

- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.15
- Installed package : libuno-purenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.15
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.15
- Installed package : libunoloader-jar_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-jar_1:6.4.7-0ubuntu0.20.04.15
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.15
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.15
- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.15

232984 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Libxslt vulnerability (USN-7357-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7357-1 advisory.

Ivan Fratric discovered that Libxslt incorrectly handled certain memory operations when handling documents. A remote attacker could use this issue to cause Libxslt to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7357-1>

Solution

Update the affected libxslt1-dev, libxslt1.1 and / or xsltproc packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:N/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

5.6 (CVSS2#AV:L/AC:H/Au:N/C:N/I:C/A:C)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-55549 |
| XREF | USN:7357-1 |

Plugin Information

Published: 2025/03/20, Modified: 2025/03/20

Plugin Output

tcp/0

- Installed package : libxslt1.1_1.1.34-4
- Fixed package : libxslt1.1_1.1.34-4ubuntu0.20.04.2

233046 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Libxslt vulnerability (USN-7361-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7361-1 advisory.

Ivan Fratric discovered that Libxslt incorrectly handled certain memory operations when handling documents. A remote attacker could use this issue to cause Libxslt to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7361-1>

Solution

Update the affected libxslt1-dev, libxslt1.1 and / or xsltproc packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:N/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

5.6 (CVSS2#AV:L/AC:H/Au:N/C:N/I:C/A:C)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-24855 |
| XREF | USN:7361-1 |
| XREF | IAVA:2025-A-0187 |

Plugin Information

Published: 2025/03/20, Modified: 2025/03/21

Plugin Output

tcp/0

- Installed package : libxslt1.1_1.1.34-4
- Fixed package : libxslt1.1_1.1.34-4ubuntu0.20.04.3

210774 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : MySQL vulnerabilities (USN-7102-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7102-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.40 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-40.html> <https://www.oracle.com/security-alerts/cpuoct2024.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7102-1>

Solution

Update the affected 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

6.8 (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-2024-21193 |
| CVE | CVE-2024-21194 |
| CVE | CVE-2024-21196 |
| CVE | CVE-2024-21197 |
| CVE | CVE-2024-21198 |
| CVE | CVE-2024-21199 |
| CVE | CVE-2024-21201 |
| CVE | CVE-2024-21212 |
| CVE | CVE-2024-21213 |
| CVE | CVE-2024-21219 |
| CVE | CVE-2024-21230 |
| CVE | CVE-2024-21231 |
| CVE | CVE-2024-21236 |
| CVE | CVE-2024-21237 |
| CVE | CVE-2024-21239 |
| CVE | CVE-2024-21241 |
| XREF | USN:7102-1 |

Plugin Information

Published: 2024/11/12, Modified: 2025/03/19

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.40-0ubuntu0.20.04.1

214820 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : MySQL vulnerabilities (USN-7245-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7245-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.41 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-41.html> <https://www.oracle.com/security-alerts/cpujan2025.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7245-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:M/C:N/I:P/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-21490 |
| CVE | CVE-2025-21491 |
| CVE | CVE-2025-21497 |
| CVE | CVE-2025-21500 |
| CVE | CVE-2025-21501 |
| CVE | CVE-2025-21503 |
| CVE | CVE-2025-21505 |
| CVE | CVE-2025-21519 |
| CVE | CVE-2025-21522 |
| CVE | CVE-2025-21523 |
| CVE | CVE-2025-21529 |
| CVE | CVE-2025-21540 |
| CVE | CVE-2025-21546 |
| CVE | CVE-2025-21555 |
| CVE | CVE-2025-21559 |
| XREF | USN:7245-1 |
| XREF | IAVA:2025-A-0272 |

Plugin Information

Published: 2025/01/30, Modified: 2025/04/18

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.41-0ubuntu0.20.04.1

211586 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Python vulnerability (USN-7116-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7116-1 advisory.

It was discovered that Python incorrectly handled quoting path names when using the venv module. A local attacker able to control virtual environments could possibly use this issue to execute arbitrary code when the virtual environment is activated.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7116-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

5.3 (CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/V:C:H/V:I:H/VA:N/SC:N/SI:N/SA:N)

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-2024-9287 |
| XREF | USN:7116-1 |

Plugin Information

Published: 2024/11/19, Modified: 2025/02/11

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.13
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.13

```
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.13

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.13

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.13
```

217185 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Raptor vulnerabilities (USN-7316-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7316-1 advisory.

It was discovered that Raptor incorrectly handled memory operations when processing certain input files. A remote attacker could possibly use this issue to cause Raptor to crash, resulting in a denial of service.

This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2020-25713)

It was discovered that Raptor incorrectly handled parsing certain tuples. A remote attacker could possibly use this issue to cause Raptor to crash, resulting in a denial of service. (CVE-2024-57822)

It was discovered that Raptor incorrectly handled parsing certain turtles. A remote attacker could use this issue to cause Raptor to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2024-57823)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7316-1>

Solution

Update the affected libraptor2-0, libraptor2-dev and / or raptor2-utils 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

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2020-25713 |
| CVE | CVE-2024-57822 |
| CVE | CVE-2024-57823 |
| XREF | USN:7316-1 |

Plugin Information

Published: 2025/03/03, Modified: 2025/03/04

Plugin Output

tcp/0

- Installed package : libraptor2-0_2.0.15-0ubuntu1
- Fixed package : libraptor2-0_2.0.15-0ubuntu1.20.04.2

216771 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : X.Org X Server vulnerabilities (USN-7299-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7299-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations. An attacker could use these issues to cause the X Server to crash, leading to a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7299-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-26594 |
| CVE | CVE-2025-26595 |
| CVE | CVE-2025-26596 |
| CVE | CVE-2025-26597 |
| CVE | CVE-2025-26598 |
| CVE | CVE-2025-26599 |
| CVE | CVE-2025-26600 |
| CVE | CVE-2025-26601 |
| XREF | USN:7299-1 |
| XREF | IAVA:2025-A-0135 |

Plugin Information

Published: 2025/02/25, Modified: 2025/02/28

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.19

```
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.19

- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.19

- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.19

- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.19
```

209906 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : X.Org X Server vulnerability (USN-7085-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7085-1 advisory.

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations in the X Keyboard Extension. An attacker could use this issue to cause the X Server to crash, leading to a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7085-1>

Solution

Update the affected 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)

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2024-9632 |
| XREF | USN:7085-1 |
| XREF | IAVA:2025-A-0135 |

Plugin Information

Published: 2024/10/30, Modified: 2025/02/28

Plugin Output

tcp/0

```
- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.18

- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
```

- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.18
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.18
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.18
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.18

213082 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : curl vulnerability (USN-7162-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7162-1 advisory.

Harry Sintonen discovered that curl incorrectly handled credentials from .netrc files when following HTTP redirects. In certain configurations, the password for the first host could be leaked to the followed-to host, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7162-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.1 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

4.9 (CVSS2#AV:N/AC:H/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2024-11053 |
| XREF | USN:7162-1 |
| XREF | IAVA:2024-A-0794-S |

Plugin Information

Published: 2024/12/17, Modified: 2025/07/31

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.25
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.25

209984 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libarchive vulnerability (USN-7087-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7087-1 advisory.

It was discovered that libarchive incorrectly handled certain RAR archive files. If a user or automated system were tricked into processing a specially crafted RAR archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7087-1>

Solution

Update the affected packages.

Risk Factor

Medium

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

6.4 (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-2024-20696 |
| XREF | USN:7087-1 |

Plugin Information

Published: 2024/10/31, Modified: 2024/10/31

Plugin Output

tcp/0

- Installed package : libarchive13_3.4.0-2ubuntu1
- Fixed package : libarchive13_3.4.0-2ubuntu1.4

216701 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libcap2 vulnerability (USN-7287-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7287-1 advisory.

Tianjia Zhang discovered the libcap2 PAM module pam_cap incorrectly handled parsing group names in the configuration file. This could result in certain users

being granted capabilities, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7287-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.2 (CVSS2#AV:L/AC:L/Au:S/C:P/I:C/A:N)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-1390 |
| XREF | USN:7287-1 |
| XREF | IAVA:2025-A-0134 |

Plugin Information

Published: 2025/02/24, Modified: 2025/02/28

Plugin Output

tcp/0

```
- Installed package : libcap2_1:2.32-1
- Fixed package : libcap2_1:2.32-1ubuntu0.2

- Installed package : libcap2-bin_1:2.32-1
- Fixed package : libcap2-bin_1:2.32-1ubuntu0.2

- Installed package : libpam-cap_1:2.32-1
- Fixed package : libpam-cap_1:2.32-1ubuntu0.2
```

234139 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7432-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7432-1 advisory.

It was discovered that libsoup could be made to read out of bounds. An attacker could possibly use this issue to cause applications using libsoup to crash, resulting in a denial of service. (CVE-2025-2784, CVE-2025-32050, CVE-2025-32052, CVE-2025-32053)

It was discovered that libsoup could be made to dereference invalid memory. An attacker could possibly use this issue to cause applications using libsoup to crash, resulting in a denial of service.
(CVE-2025-32051)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7432-1>

Solution

Update the affected 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:N/A:H)

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:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2025-2784 |
| CVE | CVE-2025-32050 |
| CVE | CVE-2025-32051 |
| CVE | CVE-2025-32052 |
| CVE | CVE-2025-32053 |
| XREF | USN:7432-1 |

Plugin Information

Published: 2025/04/10, Modified: 2025/04/10

Plugin Output

tcp/0

- Installed package : gir1.2-soup-2.4_2.70.0-1
- Fixed package : gir1.2-soup-2.4_2.70.0-1ubuntu0.2
- Installed package : libsoup-gnome2.4-1_2.70.0-1
- Fixed package : libsoup-gnome2.4-1_2.70.0-1ubuntu0.2
- Installed package : libsoup2.4-1_2.70.0-1
- Fixed package : libsoup2.4-1_2.70.0-1ubuntu0.2

210368 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : mpg123 vulnerability (USN-7092-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7092-1 advisory.

It was discovered that mpg123 incorrectly handled certain mp3 files. If a user or automated system were tricked into opening a specially crafted mp3 file, a remote attacker could use this issue to cause mpg123 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7092-1>

Solution

Update the affected 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)

References

CVE-2024-10573
XREF-USN:7092-1

Plugin Information

Published: 2024/11/05, Modified: 2024/11/05

Plugin Output

tcp/0

- Installed package : libmpg123-0_1.25.13-1
- Fixed package : libmpg123-0_1.25.13-1ubuntu0.1

218383 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : wpa_supplicant and hostapd vulnerabilities (USN-7317-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7317-1 advisory.

George Chatzisofroniou and Panayiotis Kotzanikolaou discovered that wpa_supplicant and hostapd reused encryption elements in the PKEX protocol. An attacker could possibly use this issue to impersonate a wireless access point, and obtain sensitive information. (CVE-2022-37660)

Daniel De Almeida Braga, Mohamed Sabt, and Pierre-Alain Fouque discovered that wpa_supplicant and hostapd were vulnerable to side channel attacks due to the cache access patterns. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 20.04 LTS. (CVE-2022-23303, CVE-2022-23304)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7317-1>

Solution

Update the affected 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

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2022-23303 |
| CVE | CVE-2022-23304 |
| CVE | CVE-2022-37660 |
| XREF | USN:7317-1 |

Plugin Information

Published: 2025/03/04, Modified: 2025/03/04

Plugin Output

tcp/0

- Installed package : wpasupplicant_2:2.9-1ubuntu4.1
- Fixed package : wpasupplicant_2:2.9-1ubuntu4.6

202614 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Apache HTTP Server vulnerability (USN-6902-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6902-1 advisory.

It was discovered that the Apache HTTP Server incorrectly handled certain handlers configured via AddType.
A remote attacker could possibly use this issue to obtain source code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6902-1>

Solution

Update the affected 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:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

|

References

| | |
|------|--------------------|
| CVE | CVE-2024-40725 |
| XREF | IAVA:2024-A-0411 |
| XREF | USN:6902-1 |
| XREF | IAVA:2025-A-0508-S |

Plugin Information

Published: 2024/07/18, Modified: 2025/08/12

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.21
- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.21
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.21
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.21

205629 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : GNOME Shell vulnerability (USN-6963-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6963-1 advisory.

It was discovered that GNOME Shell incorrectly opened the portal helper automatically when detecting a captive network portal. A remote attacker could possibly use this issue to load arbitrary web pages containing JavaScript, leading to resource consumption or other attacks.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6963-1>

Solution

Update the affected gnome-shell, gnome-shell-common and / or gnome-shell-extension-prefs 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

6.8 (CVSS2#AV:A/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2024-36472 |
| XREF | USN:6963-1 |

Plugin Information

Published: 2024/08/15, Modified: 2024/11/20

Plugin Output

tcp/0

- Installed package : gnome-shell_3.36.3-1ubuntu1~20.04.2
- Fixed package : gnome-shell_3.36.9-0ubuntu0.20.04.4
- Installed package : gnome-shell-common_3.36.3-1ubuntu1~20.04.2
- Fixed package : gnome-shell-common_3.36.9-0ubuntu0.20.04.4

202475 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : GTK vulnerability (USN-6899-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6899-1 advisory.

It was discovered that GTK would attempt to load modules from the current directory, contrary to expectations. If users started GTK applications from shared directories, a local attacker could use this issue to execute arbitrary code, and possibly escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6899-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.0 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.1 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.2 (CVSS2#AV:L/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-2024-6655
XREF USN:6899-1

Plugin Information

Published: 2024/07/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-gtk-3.0_3.24.20-0ubuntu1
- Fixed package : gir1.2-gtk-3.0_3.24.20-0ubuntu1.2
- Installed package : gtk-update-icon-cache_3.24.20-0ubuntu1
- Fixed package : gtk-update-icon-cache_3.24.20-0ubuntu1.2
- Installed package : gtk2-engines-pixbuf_2.24.32-4ubuntu4

- Fixed package : gtk2-engines-pixbuf_2.24.32-4ubuntu4.1
- Installed package : libgail-common_2.24.32-4ubuntu4
- Fixed package : libgail-common_2.24.32-4ubuntu4.1
- Installed package : libgail18_2.24.32-4ubuntu4
- Fixed package : libgail18_2.24.32-4ubuntu4.1
- Installed package : libgtk-3-0_3.24.20-0ubuntu1
- Fixed package : libgtk-3-0_3.24.20-0ubuntu1.2
- Installed package : libgtk-3-bin_3.24.20-0ubuntu1
- Fixed package : libgtk-3-common_3.24.20-0ubuntu1.2
- Installed package : libgtk2.0-0_2.24.32-4ubuntu4
- Fixed package : libgtk2.0-0_2.24.32-4ubuntu4.1
- Installed package : libgtk2.0-bin_2.24.32-4ubuntu4
- Fixed package : libgtk2.0-common_2.24.32-4ubuntu4.1

204922 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : MySQL vulnerabilities (USN-6934-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6934-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.39 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 24.04 LTS.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-38.html> <https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-39.html>
<https://www.oracle.com/security-alerts/cpujul2024.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6934-1>

Solution

Update the affected 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

6.8 (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-2024-20996 |
| CVE | CVE-2024-21125 |
| CVE | CVE-2024-21127 |
| CVE | CVE-2024-21129 |
| CVE | CVE-2024-21130 |
| CVE | CVE-2024-21134 |
| CVE | CVE-2024-21142 |
| CVE | CVE-2024-21162 |
| CVE | CVE-2024-21163 |
| CVE | CVE-2024-21165 |
| CVE | CVE-2024-21171 |
| CVE | CVE-2024-21173 |
| CVE | CVE-2024-21177 |
| CVE | CVE-2024-21179 |
| CVE | CVE-2024-21185 |
| XREF | USN:6934-1 |

Plugin Information

Published: 2024/07/31, Modified: 2025/03/28

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.39-0ubuntu0.20.04.1

205640 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : ORC vulnerability (USN-6964-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6964-1 advisory.

Noriko Totsuka discovered that ORC incorrectly handled certain crafted file. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6964-1>

Solution

Update the affected 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)

References

| | |
|------|----------------|
| CVE | CVE-2024-40897 |
| XREF | USN:6964-1 |

Plugin Information

Published: 2024/08/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : liborc-0.4-0_1:0.4.31-1
- Fixed package : liborc-0.4-0_1:0.4.31-1ubuntu0.1

[207282 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Python vulnerabilities \(USN-7015-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7015-1 advisory.

It was discovered that the Python email module incorrectly parsed email addresses that contain special characters. A remote attacker could possibly use this issue to bypass certain protection mechanisms.

(CVE-2023-27043)

It was discovered that Python allowed excessive backtracking while parsing certain tarfile headers. A remote attacker could possibly use this issue to cause Python to consume resources, leading to a denial of service. (CVE-2024-6232)

It was discovered that the Python email module incorrectly quoted newlines for email headers. A remote attacker could possibly use this issue to perform header injection. (CVE-2024-6923)

It was discovered that the Python http.cookies module incorrectly handled parsing cookies that contained backslashes for quoted characters. A remote attacker could possibly use this issue to cause Python to consume resources, leading to a denial of service. (CVE-2024-7592)

It was discovered that the Python zipfile module incorrectly handled certain malformed zip files. A remote attacker could possibly use this issue to cause Python to stop responding, resulting in a denial of service. (CVE-2024-8088)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7015-1>

Solution

Update the affected 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/Vl: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

4.8 (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-2023-27043 |
| CVE | CVE-2024-6232 |

| | |
|------|---------------|
| CVE | CVE-2024-6923 |
| CVE | CVE-2024-7592 |
| CVE | CVE-2024-8088 |
| XREF | USN:7015-1 |

Plugin Information

Published: 2024/09/16, Modified: 2024/09/16

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.12

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.12

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.12

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.12

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.12
```

207281 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-7012-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7012-1 advisory.

Hiroki Kurosawa discovered that curl incorrectly handled certain OCSP responses. This could result in bad certificates not being checked properly, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7012-1>

Solution

Update the affected 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: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

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)

STIG Severity

I

References

CVE

CVE-2024-8096

XREF USN:7012-1
XREF IAVA:2024-A-0571-S

Plugin Information

Published: 2024/09/16, Modified: 2025/07/31

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.24
- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.24

204952 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : snapd vulnerabilities (USN-6940-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6940-1 advisory.

Neil McPhail discovered that snapd did not properly restrict writes to the \$HOME/bin path in the AppArmor profile for snaps using the home plug. An attacker who could convince a user to install a malicious snap could use this vulnerability to escape the snap sandbox. (CVE-2024-1724)

Zeyad Gouda discovered that snapd failed to properly check the file type when extracting a snap. An attacker who could convince a user to install a malicious snap containing non-regular files could then cause snapd to block indefinitely while trying to read from such files and cause a denial of service. (CVE-2024-29068)

Zeyad Gouda discovered that snapd failed to properly check the destination of symbolic links when extracting a snap. An attacker who could convince a user to install a malicious snap containing crafted symbolic links could then cause snapd to write out the contents of the symbolic link destination into a world-readable directory. This in-turn could allow a local unprivileged user to gain access to privileged information. (CVE-2024-29069)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6940-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.2 (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.4 (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-2024-1724 |
| CVE | CVE-2024-29068 |
| CVE | CVE-2024-29069 |
| XREF | USN:6940-1 |

Plugin Information

Published: 2024/08/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.63+20.04ubuntu0.1

216431 - Ubuntu 20.04 LTS / 22.04 LTS / 24.10 : Libtasn1 vulnerability (USN-7275-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7275-1 advisory.

Bing Shi discovered that Libtasn1 inefficiently handled certificates. An attacker could possibly use this issue to increase resource utilization leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7275-1>

Solution

Update the affected libtasn1-6, libtasn1-6-dev and / or libtasn1-bin 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: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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-12133 |
| XREF | USN:7275-1 |

Plugin Information

Published: 2025/02/18, Modified: 2025/02/18

Plugin Output

tcp/0

- Installed package : libtasn1-6_4.16.0-2
- Fixed package : libtasn1-6_4.16.0-2ubuntu0.1

215238 - Ubuntu 20.04 LTS / 22.04 LTS / 24.10 : Vim vulnerability (USN-7261-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7261-1 advisory.

It was discovered that Vim incorrectly handled certain internal calls when scrolling a window. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7261-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:L/AC:H/Au:S/C:P/I:P/A:C)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-24014 |
| XREF | USN:7261-1 |
| XREF | IAVA:2025-A-0055-S |

Plugin Information

Published: 2025/02/10, Modified: 2025/08/14

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.31
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.31
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.31

181316 - Ubuntu 20.04 LTS / 22.04 LTS : FLAC vulnerability (USN-6360-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6360-1 advisory.

It was discovered that FLAC incorrectly handled encoding certain files. A remote attacker could use this issue to cause FLAC to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6360-1>

Solution

Update the affected 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
XREF

[CVE-2020-22219](#)

USN:6360-1

Plugin Information

Published: 2023/09/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libflac8_1.3.3-1build1
- Fixed package : libflac8_1.3.3-1ubuntu0.2

165011 - Ubuntu 20.04 LTS / 22.04 LTS : GDK-PixBuf vulnerability (USN-5607-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5607-1 advisory.

It was discovered that GDK-PixBuf incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5607-1>

Solution

Update the affected 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

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-2021-44648
XREF USN:5607-1

Plugin Information

Published: 2022/09/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.4
- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.4
- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.4
- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.4

163285 - Ubuntu 20.04 LTS / 22.04 LTS : HarfBuzz vulnerability (USN-5524-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5524-1 advisory.

It was discovered that HarfBuzz incorrectly handled certain glyph sizes. A remote attacker could use this issue to cause HarfBuzz to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5524-1>

Solution

Update the affected 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-2022-33068 |
| XREF | USN:5524-1 |

Plugin Information

Published: 2022/07/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libharfbuzz-icu0_2.6.4-1ubuntu4
- Fixed package : libharfbuzz-icu0_2.6.4-1ubuntu4.2
- Installed package : libharfbuzz0b_2.6.4-1ubuntu4
- Fixed package : libharfbuzz0b_2.6.4-1ubuntu4.2

168673 - Ubuntu 20.04 LTS / 22.04 LTS : Pillow vulnerabilities (USN-5777-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5777-1 advisory.

It was discovered that Pillow incorrectly handled the deletion of temporary files when using a temporary directory that contains spaces. An attacker could possibly use this issue to delete arbitrary files. This issue only affected Ubuntu 20.04 LTS. (CVE-2022-24303)

It was discovered that Pillow incorrectly handled the decompression of highly compressed GIF data. An attacker could possibly use this issue to cause Pillow to crash, resulting in a denial of service.

(CVE-2022-45198)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5777-1>

Solution

Update the affected python3-pil and / or python3-pil.imagetk 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:N/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A;P)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2022-24303 |
| CVE | CVE-2022-45198 |
| XREF | USN:5777-1 |

Plugin Information

Published: 2022/12/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : python3-pil_7.0.0-4ubuntu0.1
- Fixed package : python3-pil_7.0.0-4ubuntu0.7

173794 - Ubuntu 20.04 LTS / 22.04 LTS : Samba vulnerabilities (USN-5993-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5993-1 advisory.

Demi Marie Obenour discovered that the Samba LDAP server incorrectly handled certain confidential attribute values. A remote authenticated attacker could possibly use this issue to obtain certain sensitive information. (CVE-2023-0614)

Andrew Bartlett discovered that the Samba AD DC admin tool incorrectly sent passwords in cleartext. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-0922)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5993-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:I/I:N/A:N)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-0614 |
| CVE | CVE-2023-0922 |
| XREF | IAVA:2023-A-0167-S |
| XREF | USN:5993-1 |

Plugin Information

Published: 2023/04/03, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.15.13+dfsg-0ubuntu0.20.04.2

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.15.13+dfsg-0ubuntu0.20.04.2
```

213601 - Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerability (USN-7193-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7193-1 advisory.

Masato Kinugawa discovered that Thunderbird did not properly validate the CSP policy in the Web Compatibility extension. An attacker could potentially exploit this issue to perform a cross-site scripting attack.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7193-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------------------|
| CVE | CVE-2024-11694 |
| XREF | USN:7193-1 |
| XREF | IAVA:2024-A-0769-S |

Plugin Information

Published: 2025/01/09, Modified: 2025/01/17

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:115.18.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:115.18.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:115.18.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:115.18.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:115.18.0+build1-0ubuntu0.20.04.1

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:115.18.0+build1-0ubuntu0.20.04.1
```

173795 - Ubuntu 20.04 LTS / 22.04 LTS : ldb vulnerability (USN-5992-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5992-1 advisory.

Demi Marie Obenour discovered that ldb, when used with Samba, incorrectly handled certain confidential attribute values. A remote authenticated attacker could possibly use this issue to obtain certain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5992-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|-------------------------------|
| CVE | CVE-2023-0614 |
| XREF | USN:5992-1 |

Plugin Information

Published: 2023/04/03, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libldb2_2:2.0.10-0ubuntu0.20.04.1
- Fixed package : libldb2_2:2.4.4-0ubuntu0.20.04.2
- Installed package : python3-ldb_2:2.0.10-0ubuntu0.20.04.1
- Fixed package : python3-ldb_2:2.4.4-0ubuntu0.20.04.2

145517 - Ubuntu 20.04 LTS : Ceph vulnerabilities (USN-4706-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4706-1 advisory.

Olle Segerdahl found that ceph-mon and ceph-mgr daemons did not properly restrict access, resulting in gaining access to unauthorized resources. An authenticated user could use this vulnerability to modify the configuration and possibly conduct further attacks. (CVE-2020-10736)

Adam Mohammed found that Ceph Object Gateway was vulnerable to HTTP header injection via a CORS ExposeHeader tag. An attacker could use this to gain access or cause a crash. (CVE-2020-10753)

Ilya Dryomov found that Cephx authentication did not verify Ceph clients correctly and was then vulnerable to replay attacks in Nautilus. An attacker could use the Ceph cluster network to authenticate via a packet sniffer and perform actions. This issue is a reintroduction of CVE-2018-1128. (CVE-2020-25660)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4706-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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-2020-10736 |
| CVE | CVE-2020-10753 |
| CVE | CVE-2020-25660 |
| XREF | USN:4706-1 |

Plugin Information

Published: 2021/01/28, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libcephfs2_15.2.3-0ubuntu0.20.04.1
- Fixed package : libcephfs2_15.2.7-0ubuntu0.20.04.2

- Installed package : librados2_15.2.3-0ubuntu0.20.04.1
- Fixed package : librados2_15.2.7-0ubuntu0.20.04.2

151000 - Ubuntu 20.04 LTS : Ceph vulnerabilities (USN-4998-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4998-1 advisory.

It was discovered that in some situations Ceph logged passwords from the mgr module in clear text. An attacker could use this to expose sensitive information. (CVE-2020-25678)

Goutham Pacha Ravi, Jahson Babel, and John Garbutt discovered that user credentials in Ceph could be manipulated in certain environments. An attacker could use this to gain unintended access. (CVE-2020-27781)

It was discovered that the Ceph dashboard was susceptible to a cross-site scripting attack. An attacker could use this to expose sensitive information or gain unintended access. (CVE-2020-27839)

It was discovered that Ceph contained an authentication flaw, leading to key reuse. An attacker could use this to cause a denial of service or possibly impersonate another user. (CVE-2021-20288)

Sergey Bobrov discovered that the Ceph dashboard was susceptible to a cross-site scripting attack. An attacker could use this to expose sensitive information or gain unintended access. (CVE-2021-3509)

Sergey Bobrov discovered that Ceph's RadosGW (Ceph Object Gateway) allowed the injection of HTTP headers in responses to CORS requests. An attacker could use this to violate system integrity. (CVE-2021-3524)

It was discovered that Ceph's RadosGW (Ceph Object Gateway) did not properly handle GET requests for swift URLs in some situations, leading to an application crash. An attacker could use this to cause a denial of service. (CVE-2021-3531)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4998-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.2 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:P/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

5.1 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|-----|--------------------------------|
| CVE | CVE-2020-25678 |
| CVE | CVE-2020-27781 |

| | |
|------|----------------|
| CVE | CVE-2020-27839 |
| CVE | CVE-2021-3509 |
| CVE | CVE-2021-3524 |
| CVE | CVE-2021-3531 |
| CVE | CVE-2021-20288 |
| XREF | USN:4998-1 |

Plugin Information

Published: 2021/06/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcephfs2_15.2.3-0ubuntu0.20.04.1
- Fixed package : libcephfs2_15.2.12-0ubuntu0.20.04.1
- Installed package : librados2_15.2.3-0ubuntu0.20.04.1
- Fixed package : librados2_15.2.12-0ubuntu0.20.04.1

156633 - Ubuntu 20.04 LTS : Exiv2 regression (USN-5043-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5043-2 advisory.

USN-5043-1 fixed vulnerabilities in Exiv2. The update introduced a new regression that could cause a crash in applications using libexiv2. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5043-2>

Solution

Update the affected exiv2, libexiv2-27 and / or libexiv2-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

4.8 (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-2021-37620 |
| XREF | USN:5043-2 |

Plugin Information

Published: 2022/01/12, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libexiv2-27_0.27.2-8ubuntu2
- Fixed package : libexiv2-27_0.27.2-8ubuntu2.7

213603 - Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7191-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7191-1 advisory.

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2025-0237, CVE-2025-0239, CVE-2025-0240, CVE-2025-0242, CVE-2025-0243, CVE-2025-0247)

Irvan Kurniawan discovered that Firefox incorrectly handled memory when breaking lines in text, leading to a use-after-free vulnerability. An attacker could possibly use this issue to cause a denial of service or possibly execute arbitrary code. (CVE-2025-0238)

Nils Bars discovered that Firefox incorrectly handled memory when using JavaScript Text Segmentation. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-0241)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7191-1>

Solution

Update the affected 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

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-0237 |
| CVE | CVE-2025-0238 |
| CVE | CVE-2025-0239 |
| CVE | CVE-2025-0240 |
| CVE | CVE-2025-0241 |
| CVE | CVE-2025-0242 |
| CVE | CVE-2025-0243 |
| CVE | CVE-2025-0247 |
| XREF | USN:7191-1 |
| XREF | IAVA:2025-A-0009-S |

Plugin Information

Published: 2025/01/09, Modified: 2025/02/06

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_134.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_134.0+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_134.0+build1-0ubuntu0.20.04.1

209521 - Ubuntu 20.04 LTS : Firefox vulnerability (USN-7078-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7078-1 advisory.

Atte Kettunen discovered that Firefox did not properly validate before inserting ranges into the selection node cache. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7078-1>

Solution

Update the affected 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

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:O/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2024-9936 |
| XREF | USN:7078-1 |
| XREF | IAVA:2024-A-0663-S |

Plugin Information

Published: 2024/10/22, Modified: 2024/12/06

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_131.0.3+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_131.0.3+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_131.0.3+build1-0ubuntu0.20.04.1
```

143585 - Ubuntu 20.04 LTS : GDK-PixBuf vulnerability (USN-4663-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4663-1 advisory.

Melvin Kool discovered that the GDK-PixBuf library did not properly handle certain GIF images. If an user or automated system were tricked into opening a specially crafted GIF file, a remote attacker could use this flaw to cause GDK-PixBuf to hang, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4663-1>

Solution

Update the affected 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

4.3 (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-2020-29385 |
| XREF | USN:4663-1 |

Plugin Information

Published: 2020/12/09, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.1

- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.1

- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.1

- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.1
```

177263 - Ubuntu 20.04 LTS : GNU binutils vulnerability (USN-6160-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6160-1 advisory.

It was discovered that GNU binutils incorrectly performed bounds checking operations when parsing stabs debugging information. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6160-1>

Solution

Update the affected 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-2021-45078 |
| XREF | USN:6160-1 |

Plugin Information

Published: 2023/06/13, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : binutils_2.34-6ubuntu1
- Fixed package : binutils_2.34-6ubuntu1.6

- Installed package : binutils-common_2.34-6ubuntu1
- Fixed package : binutils-common_2.34-6ubuntu1.6

- Installed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1
- Fixed package : binutils-x86-64-linux-gnu_2.34-6ubuntu1.6

- Installed package : libbinutils_2.34-6ubuntu1
- Fixed package : libbinutils_2.34-6ubuntu1.6

- Installed package : libctf-nobfd0_2.34-6ubuntu1
- Fixed package : libctf-nobfd0_2.34-6ubuntu1.6

- Installed package : libctf0_2.34-6ubuntu1
- Fixed package : libctf0_2.34-6ubuntu1.6
```

150130 - Ubuntu 20.04 LTS : GUPnP vulnerability (USN-4970-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4970-1 advisory.

It was discovered that GUPnP incorrectly filtered local requests. If a user were tricked into visiting a malicious website, a remote attacker could possibly use this issue to perform actions against local UPnP services such as obtaining or altering sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4970-1>

Solution

Update the affected gir1.2-gupnp-1.2, libgupnp-1.2-0 and / or libgupnp-1.2-dev 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:H/A:N)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/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

4.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-2021-33516
XREF USN:4970-1

Plugin Information

Published: 2021/06/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgupnp-1.2-0_1.2.2-1
- Fixed package : libgupnp-1.2-0_1.2.3-0ubuntu0.20.04.2

140458 - Ubuntu 20.04 LTS : GnuTLS vulnerability (USN-4491-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4491-1 advisory.

It was discovered that GnuTLS incorrectly handled certain alerts when being used with TLS 1.3 servers. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4491-1>

Solution

Update the affected 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

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE-2020-24659
XREF-USN:4491-1

Plugin Information

Published: 2020/09/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls30_3.6.13-2ubuntu1.2
- Fixed package : libgnutls30_3.6.13-2ubuntu1.3

155722 - Ubuntu 20.04 LTS : ICU vulnerability (USN-5156-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5156-1 advisory.

It was discovered that ICU contains a double free issue. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5156-1>

Solution

Update the affected icu-devtools, libicu-dev and / or libicu66 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

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-2021-30535 |
| XREF | USN:5156-1 |
| XREF | IAVA:2021-A-0253-S |

Plugin Information

Published: 2021/11/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libicu66_66.1-2ubuntu2
- Fixed package : libicu66_66.1-2ubuntu2.1

153508 - Ubuntu 20.04 LTS : LibTIFF vulnerability (USN-5084-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5084-1 advisory.

It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5084-1>

Solution

Update the affected 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 |
| XREF | USN:5084-1 |

Plugin Information

Published: 2021/09/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.1.0+git191117-2build1
- Fixed package : libtiff5_4.1.0+git191117-2ubuntu0.20.04.2

155672 - Ubuntu 20.04 LTS : LibreOffice vulnerabilities (USN-5153-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5153-1 advisory.

It was discovered that LibreOffice incorrectly handled digital signatures. An attacker could possibly use this issue to create a specially crafted document that would display a validly signed indicator, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5153-1>

Solution

Update the affected 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-2021-25633 |
| CVE | CVE-2021-25634 |
| XREF | USN:5153-1 |

Plugin Information

Published: 2021/11/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.11+Lib06.4.4-0ubuntu0.20.04.1
- Fixed package : fonts-opensymbol_2:102.11+Lib06.4.7-0ubuntu0.20.04.2
- Installed package : libjuh-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libjuh-java_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libjurt-java_1:6.4.4-0ubuntu0.20.04.1

- Fixed package : libjurt-java_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-base-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-base-core_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-calc_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-calc_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-common_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-core_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-core_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-draw_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-draw_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-gnome_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gnome_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-gtk3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-gtk3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-help-common_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-common_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-help-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-de_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-help-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-gb_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-help-en-us_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-help-en-us_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-impress_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-impress_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-l10n-de_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-de_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-l10n-en-gb_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-gb_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-l10n-en-za_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-l10n-en-za_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-math_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-math_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-ogltrans_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-ogltrans_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-pdfimport_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-pdfimport_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-style-breeze_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-breeze_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-style-colibre_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-colibre_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-style-elementary_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-elementary_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-style-tango_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-style-tango_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libreoffice-writer_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libreoffice-writer_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libridl-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libridl-java_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libuno-cppu3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppu3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libuno-cppuhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-cppuhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libuno-purenvhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-purenvhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libuno-sal3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-sal3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libuno-salhelpergcc3-3_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libuno-salhelpergcc3-3_1:6.4.7-0ubuntu0.20.04.2
- Installed package : libunoloader-java_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : libunoloader-java_1:6.4.7-0ubuntu0.20.04.2
- Installed package : python3-uno_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : python3-uno_1:6.4.7-0ubuntu0.20.04.2
- Installed package : uno-libs-private_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : uno-libs-private_1:6.4.7-0ubuntu0.20.04.2

- Installed package : ure_1:6.4.4-0ubuntu0.20.04.1
- Fixed package : ure_1:6.4.7-0ubuntu0.20.04.2

173619 - Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5980-1 advisory.

It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service (memory exhaustion).
(CVE-2021-3669)

It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. (CVE-2022-2196)

Gerald Lee discovered that the USB Gadget file system implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-4382)

It was discovered that the RNDIS USB driver in the Linux kernel contained an integer overflow vulnerability. A local attacker with physical access could plug in a malicious USB device to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-23559)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5980-1>

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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:L/AC:L/Au:S/C:I/C:A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-3669 |
| CVE | CVE-2022-2196 |
| CVE | CVE-2022-4382 |
| CVE | CVE-2023-23559 |
| XREF | USN:5980-1 |

Plugin Information

Published: 2023/03/28, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-146-generic for this advisory.

158456 - Ubuntu 20.04 LTS : MariaDB vulnerabilities (USN-5305-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5305-1 advisory.

Several security issues were discovered in MariaDB and this update includes new upstream MariaDB versions to fix these issues.

MariaDB has been updated to 10.3.34 in Ubuntu 20.04 LTS and to 10.5.15 in Ubuntu 21.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5305-1>

Solution

Update the affected 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

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-46659 |
| CVE | CVE-2021-46661 |
| CVE | CVE-2021-46663 |
| CVE | CVE-2021-46664 |
| CVE | CVE-2021-46665 |
| CVE | CVE-2021-46668 |
| CVE | CVE-2022-24048 |
| CVE | CVE-2022-24050 |
| CVE | CVE-2022-24051 |
| CVE | CVE-2022-24052 |
| XREF | USN:5305-1 |

Plugin Information

Published: 2022/02/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.34-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.34-0ubuntu0.20.04.1
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.34-0ubuntu0.20.04.1
- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.34-0ubuntu0.20.04.1

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.34-0ubuntu0.20.04.1
- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.34-0ubuntu0.20.04.1
- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.34-0ubuntu0.20.04.1

155908 - Ubuntu 20.04 LTS : MariaDB vulnerability (USN-5170-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5170-1 advisory.

A security issue was discovered in MariaDB and this update includes new upstream MariaDB versions to fix the issue.

MariaDB has been updated to 10.3.32 in Ubuntu 20.04 LTS and to 10.5.13 in Ubuntu 21.04 and Ubuntu 21.10.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5170-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-35604 |
| XREF | USN:5170-1 |
| XREF | IAVA:2021-A-0487-S |

Plugin Information

Published: 2021/12/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.32-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.32-0ubuntu0.20.04.1

```
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.32-0ubuntu0.20.04.1

- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.32-0ubuntu0.20.04.1

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.32-0ubuntu0.20.04.1

- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.32-0ubuntu0.20.04.1

- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.32-0ubuntu0.20.04.1
```

144788 - Ubuntu 20.04 LTS : OpenJPEG vulnerabilities (USN-4685-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4685-1 advisory.

It was discovered that OpenJPEG incorrectly handled certain image data. An attacker could use this issue to cause OpenJPEG to crash, leading to a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4685-1>

Solution

Update the affected 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-2020-15389 |
| CVE | CVE-2020-27814 |
| CVE | CVE-2020-27823 |
| CVE | CVE-2020-27824 |
| CVE | CVE-2020-27841 |
| CVE | CVE-2020-27842 |
| CVE | CVE-2020-27843 |
| CVE | CVE-2020-27845 |
| XREF | USN:4685-1 |
| XREF | CEA-ID:CEA-2021-0025 |

Plugin Information

Published: 2021/01/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libopenjp2-7_2.3.1-1ubuntu4
- Fixed package : libopenjp2-7_2.3.1-1ubuntu4.20.04.1

147985 - Ubuntu 20.04 LTS : OpenSSH vulnerability (USN-4762-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4762-1 advisory.

It was discovered that the OpenSSH ssh-agent incorrectly handled memory. A remote attacker able to connect to the agent could use this issue to cause it to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4762-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/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

4.6 (CVSS2#AV:N/AC:H/Au:S/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2021-28041 |
| XREF | USN:4762-1 |
| XREF | IAVA:2021-A-0121-S |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.2
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.2
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.2
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.2

154053 - Ubuntu 20.04 LTS : Squashfs-Tools vulnerability (USN-5078-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5078-3 advisory.

USN-5078-1 fixed a vulnerability in Squashfs-Tools. That update was incomplete and could still result in Squashfs-Tools mishandling certain malformed SQUASHFS files. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5078-3>

Solution

Update the affected squashfs-tools package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/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

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE CVE-2021-41072
XREF USN:5078-3

Plugin Information

Published: 2021/10/13, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : squashfs-tools_1:4.4-1
- Fixed package : squashfs-tools_1:4.4-1ubuntu0.3
```

149322 - Ubuntu 20.04 LTS : Thunderbird vulnerabilities (USN-4936-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4936-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2021-23968, CVE-2021-23969, CVE-2021-23973, CVE-2021-23978)

It was discovered that Thunderbird may keep key material in memory in some circumstances. A local attacker could potentially exploit this to obtain private keys. (CVE-2021-29950)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4936-1>

Solution

Update the affected 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

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-2021-23968 |
| CVE | CVE-2021-23969 |
| CVE | CVE-2021-23973 |
| CVE | CVE-2021-23978 |
| CVE | CVE-2021-29950 |
| XREF | USN:4936-1 |

Plugin Information

Published: 2021/05/06, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : thunderbird_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird_1:78.8.1+build1~0ubuntu0.20.04.1
- Installed package : thunderbird-gnome-support_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:78.8.1+build1~0ubuntu0.20.04.1
- Installed package : thunderbird-locale-de_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:78.8.1+build1~0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:78.8.1+build1~0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:78.8.1+build1~0ubuntu0.20.04.1
- Installed package : thunderbird-locale-en-us_1:68.10.0+build1~0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:78.8.1+build1~0ubuntu0.20.04.1

150949 - Ubuntu 20.04 LTS : Thunderbird vulnerabilities (USN-4995-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4995-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass security restrictions, or execute arbitrary code. (CVE-2021-23961, CVE-2021-23981, CVE-2021-23982, CVE-2021-23987, CVE-2021-23994, CVE-2021-23998, CVE-2021-23999, CVE-2021-29945, CVE-2021-29946, CVE-2021-29967)

It was discovered that extensions could open popup windows with control of the window title in some circumstances. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to spoof a website and trick the user into providing credentials. (CVE-2021-23984)

Multiple security issues were discovered in Thunderbird's OpenPGP integration. If a user were tricked into importing a specially crafted key in some circumstances, an attacker could potentially exploit this to cause a denial of service (inability to send encrypted email) or confuse the user. (CVE-2021-23991, CVE-2021-23992, CVE-2021-23993)

A use-after-free was discovered when Responsive Design Mode was enabled. If a user were tricked into opening a specially crafted website with Responsive Design Mode enabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2021-23995)

It was discovered that Thunderbird mishandled ftp URLs with encoded newline characters. If a user were tricked into clicking on a specially crafted link, an attacker could potentially exploit this to send arbitrary FTP commands. (CVE-2021-24002)

It was discovered that Thunderbird wrote signatures to disk and read them back during verification. A local attacker could potentially exploit this to replace the data with another signature file.

(CVE-2021-29948)

It was discovered that Thunderbird might load an alternative OTR library. If a user were tricked into copying a specially crafted library to one of Thunderbird's search paths, an attacker could potentially exploit this to execute arbitrary code. (CVE-2021-29949)

It was discovered that secret keys imported into Thunderbird were stored unencrypted. A local attacker could potentially exploit this to obtain private keys. (CVE-2021-29956)

It was discovered that Thunderbird did not indicate when an inline signed or encrypted message contained additional unprotected parts. (CVE-2021-29957)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4995-1>

Solution

Update the affected 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

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-2021-23961 |
| CVE | CVE-2021-23981 |
| CVE | CVE-2021-23982 |
| CVE | CVE-2021-23984 |
| CVE | CVE-2021-23987 |

| | |
|------|--------------------|
| CVE | CVE-2021-23991 |
| CVE | CVE-2021-23992 |
| CVE | CVE-2021-23993 |
| CVE | CVE-2021-23994 |
| CVE | CVE-2021-23995 |
| CVE | CVE-2021-23998 |
| CVE | CVE-2021-23999 |
| CVE | CVE-2021-24002 |
| CVE | CVE-2021-29945 |
| CVE | CVE-2021-29946 |
| CVE | CVE-2021-29948 |
| CVE | CVE-2021-29949 |
| CVE | CVE-2021-29956 |
| CVE | CVE-2021-29957 |
| CVE | CVE-2021-29967 |
| XREF | USN:4995-1 |
| XREF | IAVA:2021-A-0051-S |
| XREF | IAVA:2021-A-0185-S |
| XREF | IAVA:2021-A-0144-S |
| XREF | IAVA:2021-A-0163-S |
| XREF | IAVA:2021-A-0246-S |
| XREF | IAVA:2021-A-0264-S |

Plugin Information

Published: 2021/06/22, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird_1:78.11.0+build1-0ubuntu0.20.04.2

- Installed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-gnome-support_1:78.11.0+build1-0ubuntu0.20.04.2

- Installed package : thunderbird-locale-de_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-de_1:78.11.0+build1-0ubuntu0.20.04.2

- Installed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en_1:78.11.0+build1-0ubuntu0.20.04.2

- Installed package : thunderbird-locale-en-gb_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-gb_1:78.11.0+build1-0ubuntu0.20.04.2

- Installed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.20.04.1
- Fixed package : thunderbird-locale-en-us_1:78.11.0+build1-0ubuntu0.20.04.2
```

165247 - Ubuntu 20.04 LTS : Vim regression (USN-5613-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5613-2 advisory.

USN-5613-1 fixed vulnerabilities in Vim. Unfortunately that update failed to include binary packages for some architectures. This update fixes that regression.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5613-2>

Solution

Update the affected 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-2022-0943 |
| CVE | CVE-2022-1154 |
| CVE | CVE-2022-1420 |
| CVE | CVE-2022-1616 |
| CVE | CVE-2022-1619 |
| CVE | CVE-2022-1620 |
| CVE | CVE-2022-1621 |
| XREF | USN:5613-2 |

Plugin Information

Published: 2022/09/19, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.9
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.9
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.9

154778 - Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5127-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5127-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5127-1>

Solution

Update the affected 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

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-2021-30846 |
| CVE | CVE-2021-30851 |
| CVE | CVE-2021-42762 |
| XREF | USN:5127-1 |

Plugin Information

Published: 2021/11/01, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.34.1-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.34.1-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.34.1-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.34.1-0ubuntu0.20.04.1

156543 - Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5213-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5213-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5213-1>

Solution

Update the affected 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:H/A:N)

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:P/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2021-30887 |
| CVE | CVE-2021-30890 |
| XREF | USN:5213-1 |
| XREF | IAVA:2021-A-0505-S |

Plugin Information

Published: 2022/01/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.34.3-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.34.3-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.34.3-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.34.3-0ubuntu0.20.04.1

158453 - Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5306-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5306-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5306-1>

Solution

Update the affected 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-2022-22589 |
| CVE | CVE-2022-22590 |
| CVE | CVE-2022-22592 |
| XREF | USN:5306-1 |

Plugin Information

Published: 2022/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.34.6-0ubuntu0.20.04.1

- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.34.6-0ubuntu0.20.04.1

- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.34.6-0ubuntu0.20.04.1

- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.34.6-0ubuntu0.20.04.1
```

140589 - Ubuntu 20.04 LTS : cryptsetup vulnerability (USN-4493-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4493-1 advisory.

It was discovered that cryptsetup incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4493-1>

Solution

Update the affected 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

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-14382 |
| XREF | USN:4493-1 |

Plugin Information

Published: 2020/09/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcryptsetup12_2:2.2.2-3ubuntu2
- Fixed package : libcryptsetup12_2:2.2.2-3ubuntu2.2

158072 - Ubuntu 20.04 LTS : cryptsetup vulnerability (USN-5286-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5286-1 advisory.

Milan Broz discovered that cryptsetup incorrectly handled LUKS2 reencryption recovery. An attacker with physical access to modify the encrypted device header may trigger the device to be unencrypted the next time it is mounted by the user.

On Ubuntu 20.04 LTS, this issue was fixed by disabling the online reencryption feature.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5286-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:P/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

3.8 (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:C/A:N)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-4122 |
| XREF | USN:5286-1 |

Plugin Information

Published: 2022/02/15, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libcryptsetup12_2:2.2.2-3ubuntu2
- Fixed package : libcryptsetup12_2:2.2.2-3ubuntu2.4

158134 - Ubuntu 20.04 LTS : libarchive vulnerabilities (USN-5291-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5291-1 advisory.

It was discovered that libarchive incorrectly handled symlinks. If a user or automated system were tricked into processing a specially crafted archive, an attacker could possibly use this issue to change modes, times, ACLs, and flags on arbitrary files. (CVE-2021-23177, CVE-2021-31566)

It was discovered that libarchive incorrectly handled certain RAR archives. If a user or automated system were tricked into processing a specially crafted RAR archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36976)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5291-1>

Solution

Update the affected libarchive-dev, libarchive-tools and / or libarchive13 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

6.8 (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-2021-23177 |
| CVE | CVE-2021-31566 |
| CVE | CVE-2021-36976 |
| XREF | USN:5291-1 |

Plugin Information

Published: 2022/02/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libarchive13_3.4.0-2ubuntu1
- Fixed package : libarchive13_3.4.0-2ubuntu1.1

159645 - Ubuntu 20.04 LTS : libarchive vulnerability (USN-5374-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5374-1 advisory.

It was discovered that libarchive incorrectly handled certain archive files. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5374-1>

Solution

Update the affected libarchive-dev, libarchive-tools and / or libarchive13 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/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

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-2022-26280 |
| XREF | USN:5374-1 |

Plugin Information

Published: 2022/04/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libarchive13_3.4.0-2ubuntu1
- Fixed package : libarchive13_3.4.0-2ubuntu1.2

142866 - Ubuntu 20.04 LTS : libmaxminddb vulnerability (USN-4631-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4631-1 advisory.

It was discovered that libmaxminddb incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause applications using libmaxminddb to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4631-1>

Solution

Update the affected libmaxminddb-dev, libmaxminddb0 and / or mddb-bin 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

5.9 (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-2020-28241
XREF-USN:4631-1

Plugin Information

Published: 2020/11/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmaxminddb0_1.4.2-0ubuntu1
- Fixed package : libmaxminddb0_1.4.2-0ubuntu1.20.04.1

152869 - Ubuntu 20.04 LTS : libssh vulnerability (USN-5053-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5053-1 advisory.

It was discovered that libssh incorrectly handled rekeying. A remote attacker could use this issue to cause libssh to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5053-1>

Solution

Update the affected 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

4.0 (CVSS2#AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

| | |
|------|-------------------------------|
| CVE | CVE-2021-3634 |
| XREF | USN:5053-1 |
| XREF | IAVA:2022-A-0041-S |

Plugin Information

Published: 2021/08/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssh-4_0.9.3-2ubuntu2
- Fixed package : libssh-4_0.9.3-2ubuntu2.2

140924 - Ubuntu 20.04 LTS : libuv vulnerability (USN-4548-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4548-1 advisory.

It was discovered that libuv incorrectly handled certain paths. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4548-1>

Solution

Update the affected libuv1 and / or libuv1-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

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|-------------------------------|
| CVE | CVE-2020-8252 |
| XREF | USN:4548-1 |
| XREF | IAVB:2020-B-0057-S |

Plugin Information

Published: 2020/09/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libuv1_1.34.2-1ubuntu1
- Fixed package : libuv1_1.34.2-1ubuntu1.1

151443 - Ubuntu 20.04 LTS : libuv vulnerability (USN-5007-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5007-1 advisory.

Eric Sesterhenn discovered that libuv incorrectly handled certain strings. An attacker could possibly use this issue to access sensitive information or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5007-1>

Solution

Update the affected libuv1 and / or libuv1-dev 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:L/I:N/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:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-22918 |
| XREF | USN:5007-1 |

Plugin Information

Published: 2021/07/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libuv1_1.34.2-1ubuntu1
- Fixed package : libuv1_1.34.2-1ubuntu1.3

211912 - Ubuntu 20.04 LTS : mpg123 vulnerability (USN-7092-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7092-2 advisory.

USN-7092-1 fixed a vulnerability in mpg123. Bastien Roucaris discovered that the fix was incomplete on Ubuntu 20.04 LTS. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7092-2>

Solution

Update the affected 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

6.8 (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-2024-10573
XREF USN:7092-2

Plugin Information

Published: 2024/11/27, Modified: 2024/11/27

Plugin Output

tcp/0

- Installed package : libmpg123-0_1.25.13-1
- Fixed package : libmpg123-0_1.25.13-1ubuntu0.2

158160 - Ubuntu 20.04 LTS : snapd vulnerabilities (USN-5292-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5292-2 advisory.

USN-5292-1 fixed vulnerabilities in snapd. This update provides the corresponding update for the riscv64 architecture.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5292-2>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

6.9 (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-2021-3155 |
| CVE | CVE-2021-4120 |
| CVE | CVE-2021-44730 |
| CVE | CVE-2021-44731 |
| XREF | USN:5292-2 |

Plugin Information

Published: 2022/02/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.54.3+20.04.1

156711 - Ubuntu 20.04 LTS : systemd vulnerability (USN-5226-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5226-1 advisory.

It was discovered that systemd-tmpfiles employed uncontrolled recursion when removing deeply nested directory hierarchies. A local attacker could exploit this to cause systemd-tmpfiles to crash or have other unspecified impacts.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5226-1>

Solution

Update the affected 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-2021-3997 |
| XREF | USN:5226-1 |

Plugin Information

Published: 2022/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss-systemd_245.4-4ubuntu3.2
- Fixed package : libnss-systemd_245.4-4ubuntu3.15
- Installed package : libpam-systemd_245.4-4ubuntu3.2
- Fixed package : libpam-systemd_245.4-4ubuntu3.15
- Installed package : libsystemd0_245.4-4ubuntu3.2
- Fixed package : libsystemd0_245.4-4ubuntu3.15
- Installed package : libudev1_245.4-4ubuntu3.2
- Fixed package : libudev1_245.4-4ubuntu3.15
- Installed package : systemd_245.4-4ubuntu3.2
- Fixed package : systemd_245.4-4ubuntu3.15
- Installed package : systemd-sysv_245.4-4ubuntu3.2
- Fixed package : systemd-sysv_245.4-4ubuntu3.15
- Installed package : systemd-timesyncd_245.4-4ubuntu3.2
- Fixed package : systemd-timesyncd_245.4-4ubuntu3.15
- Installed package : udev_245.4-4ubuntu3.2
- Fixed package : udev_245.4-4ubuntu3.15

[170179 - Ubuntu 20.04 LTS : urllib3 vulnerability \(USN-5812-1\)](#)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5812-1 advisory.

It was discovered that urllib3 incorrectly handled certain characters in URLs. A remote attacker could possibly use this issue to cause urllib3 to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5812-1>

Solution

Update the affected python3-urllib3 package.

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)

References

| | |
|------|----------------|
| CVE | CVE-2021-33503 |
| XREF | USN:5812-1 |

Plugin Information

Published: 2023/01/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.25.8-2
- Fixed package : python3-urllib3_1.25.8-2ubuntu0.2

157843 - Ubuntu 20.04 LTS : util-linux vulnerabilities (USN-5279-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5279-1 advisory.

It was discovered that util-linux incorrectly handled unmounting FUSE filesystems. A local attacker could possibly use this issue to unmount FUSE filesystems belonging to other users.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5279-1>

Solution

Update the affected 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-2021-3995 |
| CVE | CVE-2021-3996 |
| XREF | USN:5279-1 |

Plugin Information

Published: 2022/02/09, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : bsduutils_1:2.34-0.1ubuntu9
- Fixed package : bsduutils_1:2.34-0.1ubuntu9.3

- Installed package : fdisk_2.34-0.1ubuntu9
- Fixed package : fdisk_2.34-0.1ubuntu9.3

- Installed package : libblkid1_2.34-0.1ubuntu9
- Fixed package : libblkid1_2.34-0.1ubuntu9.3

- Installed package : libfdisk1_2.34-0.1ubuntu9
- Fixed package : libfdisk1_2.34-0.1ubuntu9.3

- Installed package : libmount1_2.34-0.1ubuntu9
- Fixed package : libmount1_2.34-0.1ubuntu9.3

- Installed package : libsmartcols1_2.34-0.1ubuntu9
- Fixed package : libsmartcols1_2.34-0.1ubuntu9.3

- Installed package : libuuid1_2.34-0.1ubuntu9
- Fixed package : libuuid1_2.34-0.1ubuntu9.3

- Installed package : mount_2.34-0.1ubuntu9
- Fixed package : mount_2.34-0.1ubuntu9.3

- Installed package : rfkill_2.34-0.1ubuntu9
- Fixed package : rfkill_2.34-0.1ubuntu9.3

- Installed package : util-linux_2.34-0.1ubuntu9
- Fixed package : util-linux_2.34-0.1ubuntu9.3

- Installed package : uuid-runtime_2.34-0.1ubuntu9
- Fixed package : uuid-runtime_2.34-0.1ubuntu9.3
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

| | |
|------|-------------------------------|
| CVE | CVE-1999-0524 |
| XREF | CWE:200 |

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The difference between the local and remote clocks is 1 second.

233967 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerabilities (USN-7419-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7419-1 advisory.

It was discovered that Vim incorrectly handled memory when using invalid input with the log option. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 24.04 LTS and Ubuntu 24.10. (CVE-2025-1215)

It was discovered that Vim incorrectly handled memory when redirecting certain output to the register. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-26603)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7419-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

2.4 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/V/C:N/V/I:N/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

4.2 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

3.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

1.7 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-1215 |
| CVE | CVE-2025-26603 |
| XREF | USN:7419-1 |
| XREF | IAVA:2025-A-0128-S |

Plugin Information

Published: 2025/04/07, Modified: 2025/04/17

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.32
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.32
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.32

211920 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerability (USN-7131-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7131-1 advisory.

It was discovered that Vim incorrectly handled memory when closing a buffer, leading to use-after-free. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7131-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.1 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.8 (CVSS2#AV:L/AC:H/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

2.8 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2024-47814 |
| XREF | USN:7131-1 |
| XREF | IAVA:2024-A-0618-S |

Plugin Information

Published: 2024/11/27, Modified: 2025/08/19

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.29
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.29
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.29

186711 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6543-1 advisory.

It was discovered that tar incorrectly handled extended attributes in PAX archives. An attacker could use this issue to cause tar to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6543-1>

Solution

Update the affected tar and / or tar-scripts packages.

Risk Factor

Low

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

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-2023-39804 |
| XREF | USN:6543-1 |

Plugin Information

Published: 2023/12/11, Modified: 2024/11/13

Plugin Output

tcp/0

- Installed package : tar_1.30+dfsg-7
- Fixed package : tar_1.30+dfsg-7ubuntu0.20.04.4

185569 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : procps-ng vulnerability (USN-6477-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6477-1 advisory.

It was discovered that the procps-ng ps tool incorrectly handled memory. An attacker could possibly use this issue to cause procps-ng to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6477-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

1.7 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2023-4016 |
| XREF | IAVA:2023-A-0434 |
| XREF | USN:6477-1 |

Plugin Information

Published: 2023/11/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libprocps8_2:3.3.16-1ubuntu2
- Fixed package : libprocps8_2:3.3.16-1ubuntu2.4
- Installed package : procps_2:3.3.16-1ubuntu2
- Fixed package : procps_2:3.3.16-1ubuntu2.4

180268 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : AMD Microcode vulnerability (USN-6319-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6319-1 advisory.

Daniel Trujillo, Johannes Wikner, and Kaveh Razavi discovered that some AMD processors utilising speculative execution and branch prediction may allow unauthorised memory reads via a speculative side-channel attack. A local attacker could use this to expose sensitive information, including kernel memory.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6319-1>

Solution

Update the affected amd64-microcode package.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.8 (CVSS2#AV:L/AC:H/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE [CVE-2023-20569](#)
XREF USN:6319-1

Plugin Information

Published: 2023/08/30, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : amd64-microcode_3.20191218.1ubuntu1
- Fixed package : amd64-microcode_3.20191218.1ubuntu1.2

178940 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6257-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6257-1 advisory.

It was discovered that Open VM Tools incorrectly handled certain authentication requests. A fully compromised ESXi host can force Open VM Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. (CVE-2023-20867)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6257-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.9 (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

3.6 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

2.3 (CVSS2#AV:L/AC:H/Au:M/C:P:I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:F/RL:OF/RC:C)

References

| | |
|------|---------------------------------|
| CVE | CVE-2023-20867 |
| XREF | USN:6257-1 |
| XREF | CISA-KNOWN-EXPLOITED:2023/07/14 |

Plugin Information

Published: 2023/07/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : open-vm-tools_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools_2:11.3.0-2ubuntu0~ubuntu20.04.5
- Installed package : open-vm-tools-desktop_2:11.1.0-2~ubuntu20.04.1
- Fixed package : open-vm-tools-desktop_2:11.3.0-2ubuntu0~ubuntu20.04.5

168010 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : FLAC vulnerabilities (USN-5733-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5733-1 advisory.

It was discovered that FLAC was not properly performing memory management operations, which could result in a memory leak. An attacker could possibly use this issue to cause FLAC to consume resources, leading to a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2017-6888)

It was discovered that FLAC was not properly performing bounds checking operations when decoding data. If a user or automated system were tricked into processing a specially crafted file, an attacker could possibly use this issue to expose sensitive information or to cause FLAC to crash, leading to a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-0499)

It was discovered that FLAC was not properly performing bounds checking operations when encoding data. If a user or automated system were tricked into processing a specially crafted file, an attacker could possibly use this issue to expose sensitive information or to cause FLAC to crash, leading to a denial of service. (CVE-2021-0561)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5733-1>

Solution

Update the affected 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:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2017-6888 |
| CVE | CVE-2020-0499 |
| CVE | CVE-2021-0561 |
| XREF | USN:5733-1 |

Plugin Information

Published: 2022/11/21, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libflac8_1.3.3-1build1
- Fixed package : libflac8_1.3.3-1ubuntu0.1

170651 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Kerberos vulnerabilities (USN-5828-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5828-1 advisory.

It was discovered that Kerberos incorrectly handled certain S4U2Self requests. An attacker could possibly use this issue to cause a denial of service. This issue was only addressed in Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2018-20217)

Greg Hudson discovered that Kerberos PAC implementation incorrectly handled certain parsing operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code.

(CVE-2022-42898)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5828-1>

Solution

Update the affected packages.

Risk Factor

Low

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

3.5 (CVSS2#AV:N/AC:M/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2018-20217 |
| CVE | CVE-2022-42898 |
| XREF | USN:5828-1 |

Plugin Information

Published: 2023/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : krb5-locales_1.17-6ubuntu4
- Fixed package : krb5-locales_1.17-6ubuntu4.2
- Installed package : libgssapi-krb5-2_1.17-6ubuntu4
- Fixed package : libgssapi-krb5-2_1.17-6ubuntu4.2
- Installed package : libk5crypto3_1.17-6ubuntu4
- Fixed package : libk5crypto3_1.17-6ubuntu4.2
- Installed package : libkrb5-3_1.17-6ubuntu4
- Fixed package : libkrb5-3_1.17-6ubuntu4.2
- Installed package : libkrb5support0_1.17-6ubuntu4
- Fixed package : libkrb5support0_1.17-6ubuntu4.2

162394 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5485-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5485-1 advisory.

It was discovered that some Intel processors did not completely perform cleanup actions on multi-core shared buffers. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21123)

It was discovered that some Intel processors did not completely perform cleanup actions on microarchitectural fill buffers. A local attacker could possibly use this to expose sensitive information.

(CVE-2022-21125)

It was discovered that some Intel processors did not properly perform cleanup during specific special register write operations. A local attacker could possibly use this to expose sensitive information.

(CVE-2022-21166)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5485-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2022-21123 |
| CVE | CVE-2022-21125 |
| CVE | CVE-2022-21166 |
| XREF | USN:5485-1 |

Plugin Information

Published: 2022/06/17, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-120-generic for this advisory.

164627 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerability (USN-5587-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5587-1 advisory.

Axel Chong discovered that when curl accepted and sent back cookies containing control bytes that a HTTP(S) server might return a 400 (Bad Request Error) response. A malicious cookie host could possibly use this to cause denial-of-service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5587-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.4 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

II

References

| | |
|------|------------------------------------|
| CVE | CVE-2022-35252 |
| XREF | USN:5587-1 |
| XREF | IAVA:2022-A-0350-S |

Plugin Information

Published: 2022/09/01, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libcurl3-gnutls_7.68.0-1ubuntu2.1
- Fixed package : libcurl3-gnutls_7.68.0-1ubuntu2.13

- Installed package : libcurl4_7.68.0-1ubuntu2.1
- Fixed package : libcurl4_7.68.0-1ubuntu2.13

168227 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : shadow vulnerability (USN-5745-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5745-1 advisory.

Florian Weimer discovered that shadow was not properly copying and removing user directory trees, which could lead to a race condition. A local attacker could possibly use this issue to setup a symlink attack and alter or remove directories without authorization.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5745-1>

Solution

Update the affected login, passwd and / or uidmap packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

4.1 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|-------------------------------|
| CVE | CVE-2013-4235 |
| XREF | USN:5745-1 |

Plugin Information

Published: 2022/11/28, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : login_1:4.8.1-1ubuntu5.20.04
- Fixed package : login_1:4.8.1-1ubuntu5.20.04.3
- Installed package : passwd_1:4.8.1-1ubuntu5.20.04
- Fixed package : passwd_1:4.8.1-1ubuntu5.20.04.3

162552 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5493-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5493-1 advisory.

It was discovered that the 8 Devices USB2CAN interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash).

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5493-1>

Solution

Update the affected kernel package.

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-2022-28388
XREF USN:5493-1

Plugin Information

Published: 2022/06/27, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-121-generic for this advisory.

160233 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libsepol vulnerabilities (USN-5391-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5391-1 advisory.

Nicolas looss discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36084)

It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36085)

It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affects Ubuntu 18.04 LTS,

Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2021-36086)

It was discovered that libsepol incorrectly validated certain data, leading to a heap overflow. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36087)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5391-1>

Solution

Update the affected libsepol1, libsepol1-dev and / or sepol-utils packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.0 (CVSS:3.0/E:P/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:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-36084 |
| CVE | CVE-2021-36085 |
| CVE | CVE-2021-36086 |
| CVE | CVE-2021-36087 |
| XREF | USN:5391-1 |

Plugin Information

Published: 2022/04/27, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libsepol1_3.0-1
- Fixed package : libsepol1_3.0-1ubuntu0.1
```

237709 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Apport vulnerability (USN-7545-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7545-1 advisory.

Qualys discovered that Apport incorrectly handled metadata when processing application crashes. An attacker could possibly use this issue to leak sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7545-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.8 (CVSS2#AV:L/AC:H/Au:S/C:I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE-2025-5054
USN:7545-1

Plugin Information

Published: 2025/06/03, Modified: 2025/06/03

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.28
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.28
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.28
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.28

241623 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Ghostscript vulnerabilities (USN-7623-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7623-1 advisory.

It was discovered that OpenJPEG, vendored in Ghostscript did not correctly handle large image files. If a user or system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.
(CVE-2023-39327)

Thomas Rinsma discovered that Ghostscript did not correctly handle printing certain variables. An attacker could possibly use this issue to leak sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2024-29508)

It was discovered that Ghostscript did not correctly handle loading certain libraries. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 16.04 LTS.
(CVE-2024-33871)

It was discovered that Ghostscript did not correctly handle certain memory operations. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2024-56826, CVE-2024-56827, CVE-2025-27832, CVE-2025-27835, CVE-2025-27836)

Vasileios Flengas discovered that Ghostscript did not correctly handle argument sanitization. An attacker could possibly use this issue to leak sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, Ubuntu 24.10 and Ubuntu 25.04. (CVE-2025-48708)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7623-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

1.7 (CVSS2#AV:L/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2023-39327 |
| CVE | CVE-2024-29508 |
| CVE | CVE-2024-56826 |
| CVE | CVE-2024-56827 |
| CVE | CVE-2025-27832 |
| CVE | CVE-2025-27835 |
| CVE | CVE-2025-27836 |
| CVE | CVE-2025-48708 |
| XREF | IAVB:2024-B-0074-S |
| XREF | IAVB:2025-B-0043 |
| XREF | USN:7623-1 |

Plugin Information

Published: 2025/07/09, Modified: 2025/07/09

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : ghostscript_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript_9.50~dfsg-5ubuntu4.15+esm1
- Installed package : ghostscript-x_9.50~dfsg-5ubuntu4
- Fixed package : ghostscript-x_9.50~dfsg-5ubuntu4.15+esm1
- Installed package : libgs9_9.50~dfsg-5ubuntu4
- Fixed package : libgs9_9.50~dfsg-5ubuntu4.15+esm1
- Installed package : libgs9-common_9.50~dfsg-5ubuntu4
- Fixed package : libgs9-common_9.50~dfsg-5ubuntu4.15+esm1

235341 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : LibRaw vulnerabilities (USN-7485-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7485-1 advisory.

It was discovered that LibRaw could be made to read out of bounds. An attacker could possibly use this issue to cause applications using LibRaw to crash, resulting in a denial of service. (CVE-2025-43961, CVE-2025-43962, CVE-2025-43963, CVE-2025-43964)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7485-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

2.9 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

2.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.7 (CVSS2#AV:L/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

| | |
|------|------------------|
| CVE | CVE-2025-43961 |
| CVE | CVE-2025-43962 |
| CVE | CVE-2025-43963 |
| CVE | CVE-2025-43964 |
| XREF | IAVA:2025-A-0306 |
| XREF | USN:7485-1 |

Plugin Information

Published: 2025/05/06, Modified: 2025/05/06

Plugin Output

tcp/0

- Installed package : libraw19_0.19.5-1ubuntu1
- Fixed package : libraw19_0.19.5-1ubuntu1.4

214326 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerability (USN-7213-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7213-1 advisory.

It was discovered that poppler incorrectly handled memory when opening certain PDF files. An attacker could possibly use this issue to cause denial of service or obtain sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7213-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.2 (CVSS2#AV:L/AC:L/Au:S/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-2024-56378
USN:7213-1

Plugin Information

Published: 2025/01/17, Modified: 2025/01/17

Plugin Output

tcp/0

```
- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.5

- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.5

- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.5

- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.5
```

242586 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : GDK-PixBuf vulnerabilities (USN-7662-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7662-1 advisory.

It was discovered that GDK-Pixbuf incorrectly handled certain GIF files. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 25.04, Ubuntu 24.04 LTS, Ubuntu 22.04 LTS, and

Ubuntu 20.04 LTS. (CVE-2025-6199)

It was discovered that GDK-Pixbuf incorrectly handled certain JPEG files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2025-7345)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7662-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2025-6199 |
| CVE | CVE-2025-7345 |
| XREF | USN:7662-1 |

Plugin Information

Published: 2025/07/22, Modified: 2025/07/22

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3
- Fixed package : gir1.2-gdkpixbuf-2.0_2.40.0+dfsg-3ubuntu0.5+esm1
- Installed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-0_2.40.0+dfsg-3ubuntu0.5+esm1
- Installed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-bin_2.40.0+dfsg-3ubuntu0.5+esm1
- Installed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3
- Fixed package : libgdk-pixbuf2.0-common_2.40.0+dfsg-3ubuntu0.5+esm1

207723 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Intel Microcode vulnerabilities (USN-7033-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7033-1 advisory.

It was discovered that some Intel(R) Processors did not properly restrict access to the Running Average Power Limit (RAPL) interface. This may allow a local privileged attacker to obtain sensitive information.

(CVE-2024-23984)

It was discovered that some Intel(R) Processors did not properly implement finite state machines (FSMs) in hardware logic. This may allow a local privileged attacker to cause a denial of service (system crash).

(CVE-2024-24968)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7033-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

CVSS v4.0 Base Score

6.8 (CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N)

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.7 (CVSS2#AV:L/AC:H/Au:M/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2024-23984 |
| CVE | CVE-2024-24968 |
| XREF | USN:7033-1 |

Plugin Information

Published: 2024/09/25, Modified: 2024/09/25

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20240910.0ubuntu0.20.04.1

207996 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerability (USN-7048-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7048-1 advisory.

Suyue Guo discovered that Vim incorrectly handled memory when flushing the typeahead buffer, leading to heap-buffer-overflow. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7048-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.5 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

3.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.7 (CVSS2#AV:L/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:O/RC:C)

STIG Severity

I

References

| | |
|------|------------------------------------|
| CVE | CVE-2024-43802 |
| XREF | IAVA:2024-A-0526-S |
| XREF | USN:7048-1 |

Plugin Information

Published: 2024/10/01, Modified: 2024/10/01

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.25
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.25
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.25

143584 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Aptdaemon vulnerabilities (USN-4664-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4664-1 advisory.

Kevin Backhouse discovered that Aptdaemon incorrectly handled certain properties. A local attacker could use this issue to test for the presence of local files. (CVE-2020-16128)

Kevin Backhouse discovered that Aptdaemon incorrectly handled permission checks. A local attacker could possibly use this issue to cause a denial of service. (CVE-2020-27349)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4664-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.3 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2020-16128 |
| CVE | CVE-2020-27349 |
| XREF | USN:4664-1 |

Plugin Information

Published: 2020/12/09, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : aptdaemon_1.1.1+bzr982-0ubuntu32.1
- Fixed package : aptdaemon_1.1.1+bzr982-0ubuntu32.3
- Installed package : aptdaemon-data_1.1.1+bzr982-0ubuntu32.1
- Fixed package : aptdaemon-data_1.1.1+bzr982-0ubuntu32.3
- Installed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu32.1
- Fixed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu32.3
- Installed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu32.1
- Fixed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu32.3

140784 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Aptdaemon vulnerability (USN-4537-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4537-1 advisory.

Vaisha Bernard discovered that Aptdaemon incorrectly handled the Locale property. A local attacker could use this issue to test for the presence of local files.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4537-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.0 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2020-15703 |
| XREF | USN:4537-1 |

Plugin Information

Published: 2020/09/24, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : aptdaemon_1.1.1+bzr982-0ubuntu32.1
- Fixed package : aptdaemon_1.1.1+bzr982-0ubuntu32.2
- Installed package : aptdaemon-data_1.1.1+bzr982-0ubuntu32.1
- Fixed package : aptdaemon-data_1.1.1+bzr982-0ubuntu32.2
- Installed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu32.1
- Fixed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu32.2
- Installed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu32.1
- Fixed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu32.2

148987 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : File Roller vulnerability (USN-4927-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4927-1 advisory.

It was discovered that File Roller incorrectly handled symlinks. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4927-1>

Solution

Update the affected file-roller package.

Risk Factor

Low

CVSS v3.0 Base Score

3.9 (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L)

CVSS v3.0 Temporal Score

3.5 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:L/AC:H/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|-----|----------------|
| CVE | CVE-2020-36314 |
|-----|----------------|

XREF

USN:4927-1

Plugin Information

Published: 2021/04/26, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : file-roller_3.36.2-0ubuntu1
- Fixed package : file-roller_3.36.3-0ubuntu1.1

142731 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4628-1 advisory.

Moritz Lipp, Michael Schwarz, Andreas Kogler, David Oswald, Catherine Easdon, Claudio Canella, and Daniel Gruss discovered that the Intel Running Average Power Limit (RAPL) feature of some Intel processors allowed a side-channel attack based on power consumption measurements. A local attacker could possibly use this to expose sensitive information. (CVE-2020-8695)

Ezra Caltum, Joseph Nuzman, Nir Shildan and Ofir Joseff discovered that some Intel(R) Processors did not properly remove sensitive information before storage or transfer in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2020-8696)

Ezra Caltum, Joseph Nuzman, Nir Shildan and Ofir Joseff discovered that some Intel(R) Processors did not properly isolate shared resources in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2020-8698)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4628-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2020-8695 |
| CVE | CVE-2020-8696 |
| CVE | CVE-2020-8698 |
| XREF | USN:4628-1 |

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20201110.0ubuntu0.20.04.1
```

142721 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4627-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4627-1 advisory.

Moritz Lipp, Michael Schwarz, Andreas Kogler, David Oswald, Catherine Easdon, Claudio Canella, and Daniel Gruss discovered that the Intel Running Average Power Limit (RAPL) driver in the Linux kernel did not properly restrict access to power data. A local attacker could possibly use this to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4627-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2020-8694 |
| XREF | USN:4627-1 |

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-53-generic for this advisory.
```

183597 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PackageKit vulnerabilities (USN-4538-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4538-1 advisory.

Vaisha Bernard discovered that PackageKit incorrectly handled certain methods. A local attacker could use this issue to learn the MIME type of any file on the system. (CVE-2020-16121)

Sami Niemimki discovered that PackageKit incorrectly handled local deb packages. A local user could possibly use this issue to install untrusted packages, contrary to expectations. (CVE-2020-16122)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4538-1>

Solution

Update the affected packages.

Risk Factor

Low

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

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-16121 |
| CVE | CVE-2020-16122 |
| XREF | USN:4538-1 |

Plugin Information

Published: 2023/10/20, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : gir1.2-packagekitglib-1.0_1.1.13-2ubuntu1
- Fixed package : gir1.2-packagekitglib-1.0_1.1.13-2ubuntu1.1
- Installed package : gstreamer1.0-packagekit_1.1.13-2ubuntu1
- Fixed package : gstreamer1.0-packagekit_1.1.13-2ubuntu1.1
- Installed package : libpackagekit-glib2-18_1.1.13-2ubuntu1
- Fixed package : libpackagekit-glib2-18_1.1.13-2ubuntu1.1
- Installed package : packagekit_1.1.13-2ubuntu1
- Fixed package : packagekit_1.1.13-2ubuntu1.1
- Installed package : packagekit-tools_1.1.13-2ubuntu1
- Fixed package : packagekit-tools_1.1.13-2ubuntu1.1

143214 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PulseAudio vulnerability (USN-4640-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4640-1 advisory.

James Henstridge discovered that an Ubuntu-specific patch caused PulseAudio to incorrectly handle snap client connections. An attacker could possibly use this to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4640-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE
XREF
CVE-2020-16123
USN:4640-1

Plugin Information

Published: 2020/11/24, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libpulse-mainloop-glib0_1:13.99.1-1ubuntu3.5
- Fixed package : libpulse-mainloop-glib0_1:13.99.1-1ubuntu3.8

- Installed package : libpulse0_1:13.99.1-1ubuntu3.5
- Fixed package : libpulse0_1:13.99.1-1ubuntu3.8

- Installed package : libpulsedsp_1:13.99.1-1ubuntu3.5
- Fixed package : libpulsedsp_1:13.99.1-1ubuntu3.8

- Installed package : pulseaudio_1:13.99.1-1ubuntu3.5
- Fixed package : pulseaudio_1:13.99.1-1ubuntu3.8

- Installed package : pulseaudio-module-bluetooth_1:13.99.1-1ubuntu3.5
- Fixed package : pulseaudio-module-bluetooth_1:13.99.1-1ubuntu3.8

- Installed package : pulseaudio-utils_1:13.99.1-1ubuntu3.5
- Fixed package : pulseaudio-utils_1:13.99.1-1ubuntu3.8
```

139568 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Software Properties vulnerability (USN-4457-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4457-1 advisory.

Jason A. Donenfeld discovered that Software Properties incorrectly filtered certain escape sequences when displaying PPA descriptions. If a user were tricked into adding an arbitrary PPA, a remote attacker could possibly manipulate the screen.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4457-1>

Solution

Update the affected 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:H/A:N)

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:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2020-15709
XREF USN:4457-1

Plugin Information

Published: 2020/08/13, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : python3-software-properties_0.98.9.1
- Fixed package : python3-software-properties_0.98.9.2

- Installed package : software-properties-common_0.98.9.1
- Fixed package : software-properties-common_0.98.9.2

- Installed package : software-properties-gtk_0.98.9.1
- Fixed package : software-properties-gtk_0.98.9.2
```

139371 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ppp vulnerability (USN-4451-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4451-1 advisory.

Thomas Chauchefoin working with Trend Micros Zero Day Initiative, discovered that ppp incorrectly handled module loading. A local attacker could use this issue to load arbitrary kernel modules and possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4451-1>

Solution

Update the affected ppp, ppp-dev and / or ppp-udeb 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:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:O/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-15704 |
| XREF | USN:4451-1 |

Plugin Information

Published: 2020/08/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ppp_2.4.7-2+4.1ubuntu5
- Fixed package : ppp_2.4.7-2+4.1ubuntu5.1

144015 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-apt vulnerability (USN-4668-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4668-1 advisory.

Kevin Backhouse discovered that python-apt incorrectly handled resources. A local attacker could possibly use this issue to cause python-apt to consume resources, leading to a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4668-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

2.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

2.5 (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-2020-27351 |
| XREF | USN:4668-1 |

Plugin Information

Published: 2020/12/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python-apt-common_2.0.0ubuntu0.20.04.1
- Fixed package : python-apt-common_2.0.0ubuntu0.20.04.2
- Installed package : python3-apt_2.0.0ubuntu0.20.04.1
- Fixed package : python3-apt_2.0.0ubuntu0.20.04.2

240097 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Python vulnerabilities (USN-7570-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7570-1 advisory.

It was discovered that Python incorrectly handled certain unicode characters during decoding. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-4516)

It was discovered that Python incorrectly handled unicode encoding of email headers with list separators in folded lines. An attacker could possibly use this issue to expose sensitive information. (CVE-2025-1795)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7570-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

5.9 (CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:N/Vl:N/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:N/AC:H/Au:S/C:P:I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2025-1795 |
| CVE | CVE-2025-4516 |
| XREF | USN:7570-1 |

Plugin Information

Published: 2025/06/17, Modified: 2025/06/17

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.18+esm1
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.18+esm1
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.18+esm1
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.18+esm1
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.18+esm1

234994 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : poppler vulnerabilities (USN-7471-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7471-1 advisory.

It was discovered that poppler did not properly verify adbe.pkcs7.sha1 signatures in PDF documents. An attacker could possibly use this issue to create documents with forged signatures that are treated as legitimately signed.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7471-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.8 (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:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-43903 |
| XREF | USN:7471-1 |
| XREF | IAVB:2025-B-0070 |

Plugin Information

Published: 2025/04/29, Modified: 2025/05/09

Plugin Output

tcp/0

- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.7
- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.7
- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.7
- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.7

149907 - Ubuntu 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4965-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4965-1 advisory.

Maik Mnch discovered that Apport incorrectly handled certain information gathering operations. A local attacker could use these issues to read and write arbitrary files as an administrator, and possibly escalate privileges.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4965-1>

Solution

Update the affected packages.

Risk Factor

Low

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

6.4 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.6 (CVSS2#AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

2.8 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|-----|----------------|
| CVE | CVE-2021-32547 |
| CVE | CVE-2021-32548 |
| CVE | CVE-2021-32549 |
| CVE | CVE-2021-32550 |

| | |
|------|----------------|
| CVE | CVE-2021-32551 |
| CVE | CVE-2021-32552 |
| CVE | CVE-2021-32553 |
| CVE | CVE-2021-32554 |
| CVE | CVE-2021-32555 |
| CVE | CVE-2021-32556 |
| CVE | CVE-2021-32557 |
| XREF | USN:4965-1 |

Plugin Information

Published: 2021/05/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.18
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.18
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.18
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.18

151452 - Ubuntu 18.04 LTS / 20.04 LTS : Avahi vulnerabilities (USN-5008-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5008-1 advisory.

Thomas Kremer discovered that Avahi incorrectly handled termination signals on the Unix socket. A local attacker could possibly use this issue to cause Avahi to hang, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-3468)

It was discovered that Avahi incorrectly handled certain hostnames. A local attacker could possibly use this issue to cause Avahi to crash, resulting in a denial of service. This issue only affected Ubuntu 20.10 and Ubuntu 21.04. (CVE-2021-3502)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5008-1>

Solution

Update the affected 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

5.0 (CVSS:3.0/E:P/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:POC/RL:OF/RC:C)

References

CVE CVE-XREF
CVE-2021-3468
CVE-2021-3502
USN:5008-1

Plugin Information

Published: 2021/07/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : avahi-autoipd_0.7-4ubuntu7
- Fixed package : avahi-autoipd_0.7-4ubuntu7.1

- Installed package : avahi-daemon_0.7-4ubuntu7
- Fixed package : avahi-daemon_0.7-4ubuntu7.1

- Installed package : avahi-utils_0.7-4ubuntu7
- Fixed package : avahi-utils_0.7-4ubuntu7.1

- Installed package : libavahi-client3_0.7-4ubuntu7
- Fixed package : libavahi-client3_0.7-4ubuntu7.1

- Installed package : libavahi-common-data_0.7-4ubuntu7
- Fixed package : libavahi-common-data_0.7-4ubuntu7.1

- Installed package : libavahi-common3_0.7-4ubuntu7
- Fixed package : libavahi-common3_0.7-4ubuntu7.1

- Installed package : libavahi-core7_0.7-4ubuntu7
- Fixed package : libavahi-core7_0.7-4ubuntu7.1

- Installed package : libavahi-glib1_0.7-4ubuntu7
- Fixed package : libavahi-glib1_0.7-4ubuntu7.1

- Installed package : libavahi-ui-gtk3-0_0.7-4ubuntu7
- Fixed package : libavahi-ui-gtk3-0_0.7-4ubuntu7.1
```

150030 - Ubuntu 18.04 LTS / 20.04 LTS : DHCP vulnerability (USN-4969-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4969-1 advisory.

Jon Franklin and Paweł Wieczorkiewicz discovered that DHCP incorrectly handled lease file parsing. A remote attacker could possibly use this issue to cause DHCP to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4969-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

7.4 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/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

3.3 (CVSS2#AV:A/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

2.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-25217 |
| XREF | USN:4969-1 |

Plugin Information

Published: 2021/05/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `isc-dhcp-client_4.4.1-2.1ubuntu5`
- Fixed package : `isc-dhcp-client_4.4.1-2.1ubuntu5.20.04.2`
- Installed package : `isc-dhcp-common_4.4.1-2.1ubuntu5`
- Fixed package : `isc-dhcp-common_4.4.1-2.1ubuntu5.20.04.2`

[146436 - Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar vulnerability \(USN-4733-1\)](#)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4733-1 advisory.

Yiit Can Ylmaz discovered that GNOME Autoar could extract files outside of the intended directory. If a user were tricked into extracting a specially crafted archive, a remote attacker could create files in arbitrary locations, possibly leading to code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4733-1>

Solution

Update the affected 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: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

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-36241 |
| XREF | USN:4733-1 |

Plugin Information

Published: 2021/02/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnome-autoar-0_0_0.2.3-2
- Fixed package : libgnome-autoar-0_0_0.2.3-2ubuntu0.1

149332 - Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar vulnerability (USN-4937-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4937-1 advisory.

Ondrej Holý discovered that GNOME Autoar could extract files outside of the intended directory. If a user were tricked into extracting a specially crafted archive, a remote attacker could create files in arbitrary locations, possibly leading to code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4937-1>

Solution

Update the affected 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:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-28650 |
| XREF | USN:4937-1 |

Plugin Information

Published: 2021/05/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnome-autoar-0_0_0.2.3-2
- Fixed package : libgnome-autoar-0_0_0.2.3-2ubuntu0.3

149521 - Ubuntu 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-3)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4628-3 advisory.

USN-4628-1 provided updated Intel Processor Microcode for various processor types.

This update provides the corresponding updates for some additional processor types.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4628-3>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|-------------------------------|
| CVE | CVE-2020-8695 |
| CVE | CVE-2020-8696 |
| CVE | CVE-2020-8698 |
| XREF | USN:4628-3 |

Plugin Information

Published: 2021/05/17, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : `intel-microcode_3.20200609.0ubuntu0.20.04.2`
- Fixed package : `intel-microcode_3.20210216.0ubuntu0.20.04.1`

160025 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5384-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5384-1 advisory.

It was discovered that the UDF file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious UDF image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2022-0617)

Lyu Tao discovered that the NFS implementation in the Linux kernel did not properly handle requests to open a directory on a regular file. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-24448)

It was discovered that the YAM AX.25 device driver in the Linux kernel did not properly deallocate memory in some error conditions. A local privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2022-24959)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5384-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.0 (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)

References

| | |
|------|----------------|
| CVE | CVE-2022-0617 |
| CVE | CVE-2022-24448 |
| CVE | CVE-2022-24959 |
| XREF | USN:5384-1 |

Plugin Information

Published: 2022/04/21, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-109-generic for this advisory.

165287 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5622-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5622-1 advisory.

It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33655)

Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information. (CVE-2022-1012, CVE-2022-32296)

Norbert Slusarek discovered that a race condition existed in the perf subsystem in the Linux kernel, resulting in a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1729)

It was discovered that the device-mapper verity (dm-verity) driver in the Linux kernel did not properly verify targets being loaded into the device-mapper table. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2503)

Domingo Dirutigliano and Nicola Guerrera discovered that the netfilter subsystem in the Linux kernel did not properly handle rules that truncated packets below the packet header size. When such rules are in place, a remote attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-36946)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5622-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

8.2 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H)

CVSS v3.0 Temporal Score

7.4 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-33655 |
| CVE | CVE-2022-1012 |
| CVE | CVE-2022-1729 |
| CVE | CVE-2022-2503 |
| CVE | CVE-2022-32296 |
| CVE | CVE-2022-36946 |
| XREF | USN:5622-1 |

Plugin Information

Published: 2022/09/21, Modified: 2024/08/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-126-generic for this advisory.

166012 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5668-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5668-1 advisory.

It was discovered that the BPF verifier in the Linux kernel did not properly handle internal data structures. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2021-4159)

It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 (V4L2) implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-20369)

Duoming Zhou discovered that race conditions existed in the timer handling implementation of the Linux kernel's Rose X.25 protocol layer, resulting in use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-2318)

Roger Pau Monn discovered that the Xen virtual block driver in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-26365)

Pawan Kumar Gupta, Alyssa Milburn, Amit Peled, Shani Rehana, Nir Shildan and Ariel Sabba discovered that some Intel processors with Enhanced Indirect Branch Restricted Speculation (eIBRS) did not properly handle RET instructions after a VM exits. A local attacker could potentially use this to expose sensitive information. (CVE-2022-26373)

Eric Biggers discovered that a use-after-free vulnerability existed in the io_uring subsystem in the Linux kernel. A local attacker could possibly use this to cause a

denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3176)

Roger Pau Monn discovered that the Xen paravirtualization frontend in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-33740)

It was discovered that the Xen paravirtualization frontend in the Linux kernel incorrectly shared unrelated data when communicating with certain backends. A local attacker could use this to cause a denial of service (guest crash) or expose sensitive information (guest kernel memory). (CVE-2022-33741, CVE-2022-33742)

Oleksandr Tyshchenko discovered that the Xen paravirtualization platform in the Linux kernel on ARM platforms contained a race condition in certain situations. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2022-33744)

It was discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a reference counting error. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-36879)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5668-1>

Solution

Update the affected kernel package.

Risk Factor

Low

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

3.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2021-4159 |
| CVE | CVE-2022-2318 |
| CVE | CVE-2022-3176 |
| CVE | CVE-2022-20369 |
| CVE | CVE-2022-26365 |
| CVE | CVE-2022-26373 |
| CVE | CVE-2022-33740 |
| CVE | CVE-2022-33741 |
| CVE | CVE-2022-33742 |
| CVE | CVE-2022-33744 |
| CVE | CVE-2022-36879 |
| XREF | USN:5668-1 |

Plugin Information

Published: 2022/10/11, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-128-generic for this advisory.

167771 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5728-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5728-1 advisory.

Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)

It was discovered that a race condition existed in the memory address space accounting implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41222)

It was discovered that a race condition existed in the instruction emulator of the Linux kernel on Arm 64-bit systems. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-20422)

It was discovered that the KVM implementation in the Linux kernel did not properly handle virtual CPUs without APICs in certain situations. A local attacker could possibly use this to cause a denial of service (host system crash). (CVE-2022-2153)

Hao Sun and Jiacheng Xu discovered that the NILFS file system implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2978)

Johannes Wikner and Kaveh Razavi discovered that for some Intel x86-64 processors, the Linux kernel's protections against speculative branch target injection attacks were insufficient in some circumstances. A local attacker could possibly use this to expose sensitive information. (CVE-2022-29901)

Abhishek Shah discovered a race condition in the PF_KEYv2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3028)

It was discovered that the Netlink device interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability with some network device drivers. A local attacker with admin access to the network device could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3625)

It was discovered that the IDT 77252 ATM PCI device driver in the Linux kernel did not properly remove any pending timers during device exit, resulting in a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-3635)

Xingyuan Mo and Gengjia Chen discovered that the Promise SuperTrak EX storage controller driver in the Linux kernel did not properly handle certain structures. A local attacker could potentially use this to expose sensitive information (kernel memory). (CVE-2022-40768)

Snke Huster discovered that a use-after-free vulnerability existed in the WiFi driver stack in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42719)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5728-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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

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)

References

| | |
|-----|---------------|
| CVE | CVE-2022-2153 |
| CVE | CVE-2022-2978 |
| CVE | CVE-2022-3028 |
| CVE | CVE-2022-3625 |

| | |
|------|----------------|
| CVE | CVE-2022-3635 |
| CVE | CVE-2022-20422 |
| CVE | CVE-2022-29901 |
| CVE | CVE-2022-40768 |
| CVE | CVE-2022-41222 |
| CVE | CVE-2022-42703 |
| CVE | CVE-2022-42719 |
| XREF | USN:5728-1 |

Plugin Information

Published: 2022/11/17, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-132-generic for this advisory.

150857 - Ubuntu 18.04 LTS / 20.04 LTS : Nettle vulnerabilities (USN-4990-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4990-1 advisory.

It was discovered that Nettle incorrectly handled RSA decryption. A remote attacker could possibly use this issue to cause Nettle to crash, resulting in a denial of service. (CVE-2021-3580)

It was discovered that Nettle incorrectly handled certain padding oracles. A remote attacker could possibly use this issue to perform a variant of the Bleichenbacher attack. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-16869)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4990-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

5.7 (CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:N)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2018-16869 |
| CVE | CVE-2021-3580 |
| XREF | USN:4990-1 |

Plugin Information

Published: 2021/06/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libhogweed5_3.5.1+really3.5.1-2
 - Fixed package : libhogweed5_3.5.1+really3.5.1-2ubuntu0.2
-
- Installed package : libnettle7_3.5.1+really3.5.1-2
 - Fixed package : libnettle7_3.5.1+really3.5.1-2ubuntu0.2

152143 - Ubuntu 18.04 LTS / 20.04 LTS : PEAR vulnerability (USN-5027-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5027-1 advisory.

It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5027-1>

Solution

Update the affected php-pear package.

Risk Factor

Low

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

6.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE
XREF

CVE-2021-32610
USN:5027-1

Plugin Information

Published: 2021/07/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : php-pear_1:1.10.9+submodules+notgz-1
- Fixed package : php-pear_1:1.10.9+submodules+notgz-1ubuntu0.20.04.3

152230 - Ubuntu 18.04 LTS / 20.04 LTS : Perl DBI module vulnerabilities (USN-5030-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5030-1 advisory.

It was discovered that the Perl DBI module incorrectly opened files outside of the folder specified in the data source name. A remote attacker could possibly use this issue to obtain sensitive information.

(CVE-2014-10402)

It was discovered that the Perl DBI module incorrectly handled certain long strings. A local attacker could possibly use this issue to cause the DBI module to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-14393)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5030-1>

Solution

Update the affected libdbi-perl package.

Risk Factor

Low

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

6.4 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.6 (CVSS2#AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

2.8 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2014-10402 |
| CVE | CVE-2020-14393 |
| XREF | USN:5030-1 |

Plugin Information

Published: 2021/08/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libdbi-perl_1.643-1
- Fixed package : libdbi-perl_1.643-1ubuntu0.1

148007 - Ubuntu 18.04 LTS / 20.04 LTS : libzstd vulnerabilities (USN-4760-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4760-1 advisory.

It was discovered that libzstd incorrectly handled file permissions. A local attacker could possibly use this issue to access certain files, contrary to expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4760-1>

Solution

Update the affected 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: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

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|--------------------------------|
| CVE | CVE-2021-24031 |
| CVE | CVE-2021-24032 |
| XREF | USN:4760-1 |

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libzstd1_1.4.4+dfsg-3
- Fixed package : libzstd1_1.4.4+dfsg-3ubuntu0.1

195216 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6768-1 advisory.

Alicia Boya Garca discovered that GLib incorrectly handled signal subscriptions. A local attacker could use this issue to spoof D-Bus signals resulting in a variety of impacts including possible privilege escalation.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6768-1>

Solution

Update the affected 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](#)
XREF USN:6768-1

Plugin Information

Published: 2024/05/09, Modified: 2025/06/19

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-0_2.64.6-1~ubuntu20.04.7
- Installed package : libglib2.0-bin_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-bin_2.64.6-1~ubuntu20.04.7
- Installed package : libglib2.0-data_2.64.3-1~ubuntu20.04.1
- Fixed package : libglib2.0-data_2.64.6-1~ubuntu20.04.7

[235159 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : MySQL vulnerabilities \(USN-7479-1\)](#)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7479-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 8.0.42 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 24.04 LTS, and Ubuntu 24.10. Ubuntu 25.04 has been updated to MySQL 8.4.5.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-42.html> <https://dev.mysql.com/doc/relnotes/mysql/8.4/en/news-8-4-5.html>
<https://www.oracle.com/security-alerts/cpuapr2025.html>

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7479-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

3.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.7 (CVSS2#AV:L/AC:H/Au:M/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-2025-21574
CVE-2025-21575
CVE-2025-21577
CVE-2025-21579
CVE-2025-21580
CVE-2025-21581
CVE-2025-21584
CVE-2025-21585
CVE-2025-21588
CVE-2025-30681
CVE-2025-30682
CVE-2025-30683
CVE-2025-30684
CVE-2025-30685
CVE-2025-30687
CVE-2025-30688
CVE-2025-30689
CVE-2025-30693
CVE-2025-30695
CVE-2025-30696
CVE-2025-30699
CVE-2025-30703
CVE-2025-30704
CVE-2025-30705
CVE-2025-30715
CVE-2025-30721
CVE-2025-30722
XREF USN:7479-1

Plugin Information

Published: 2025/05/05, Modified: 2025/05/05

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.42-0ubuntu0.20.04.1

234810 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : OpenSSH vulnerability (USN-7457-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7457-1 advisory.

It was discovered that OpenSSH incorrectly handled the DisableForwarding directive. The directive would fail to disable X11 and agent forwarding, contrary to documentation and expectations.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7457-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.8 (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:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|----------------------------------|
| CVE | CVE-2025-32728 |
| XREF | IAVA:2025-A-0258 |
| XREF | USN:7457-1 |

Plugin Information

Published: 2025/04/24, Modified: 2025/04/24

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.13
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-server_1:8.2p1-4ubuntu0.13
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.13
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.13

[234800 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libarchive vulnerabilities \(USN-7454-1\)](#)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7454-1 advisory.

It was discovered that the libarchive bsdunzip utility incorrectly handled certain ZIP archive files. If a user or automated system were tricked into processing a specially crafted ZIP archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 24.04 LTS, Ubuntu 24.10, and Ubuntu 25.04. (CVE-2025-1632)

It was discovered that libarchive incorrectly handled certain TAR archive files. If a user or automated system were tricked into processing a specially crafted TAR archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2025-25724)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7454-1>**Solution**

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

4.8 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/C:N/V:I:N/VA:L/SC:N/SI:N/SA:N)

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

1.7 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|------------------|
| CVE | CVE-2025-1632 |
| CVE | CVE-2025-25724 |
| XREF | IAVA:2024-A-0834 |
| XREF | USN:7454-1 |

Plugin Information

Published: 2025/04/24, Modified: 2025/04/24

Plugin Output

tcp/0

- Installed package : libarchive13_3.4.0-2ubuntu1
- Fixed package : libarchive13_3.4.0-2ubuntu1.5

238067 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : systemd vulnerability (USN-7559-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7559-1 advisory.

Qualys discovered that systemd incorrectly handled metadata when processing application crashes. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7559-1>**Solution**

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

4.8 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

3.2 (CVSS2#AV:L/AC:L/Au:S/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

2.5 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2025-4598 |
| XREF | USN:7559-1 |

Plugin Information

Published: 2025/06/10, Modified: 2025/06/11

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

- Installed package : libnss-systemd_245.4-4ubuntu3.2
- Fixed package : libnss-systemd_245.4-4ubuntu3.24+esm1
- Installed package : libpam-systemd_245.4-4ubuntu3.2
- Fixed package : libpam-systemd_245.4-4ubuntu3.24+esm1
- Installed package : libsystemd0_245.4-4ubuntu3.2
- Fixed package : libsystemd0_245.4-4ubuntu3.24+esm1
- Installed package : libudev1_245.4-4ubuntu3.2
- Fixed package : libudev1_245.4-4ubuntu3.24+esm1
- Installed package : systemd_245.4-4ubuntu3.2
- Fixed package : systemd_245.4-4ubuntu3.24+esm1
- Installed package : systemd-sysv_245.4-4ubuntu3.2
- Fixed package : systemd-sysv_245.4-4ubuntu3.24+esm1
- Installed package : systemd-timesyncd_245.4-4ubuntu3.2
- Fixed package : systemd-timesyncd_245.4-4ubuntu3.24+esm1
- Installed package : udev_245.4-4ubuntu3.2
- Fixed package : udev_245.4-4ubuntu3.24+esm1

233821 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GnuPG vulnerability (USN-7412-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7412-1 advisory.

It was discovered that GnuPG incorrectly handled importing keys with certain crafted subkey data. If a user or automated system were tricked into importing a specially crafted key, a remote attacker may prevent users from importing other keys in the future.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7412-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

2.7 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

2.4 (CVSS:3.0/E:U/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:U/RL:OF/RC:C)

References

CVE-2025-30258
XREF USN:7412-1

Plugin Information

Published: 2025/04/03, Modified: 2025/04/03

Plugin Output

tcp/0

- Installed package : dirmngr_2.2.19-3ubuntu2
- Fixed package : dirmngr_2.2.19-3ubuntu2.4
- Installed package : gnupg_2.2.19-3ubuntu2
- Fixed package : gnupg_2.2.19-3ubuntu2.4
- Installed package : gnupg-110n_2.2.19-3ubuntu2
- Fixed package : gnupg-110n_2.2.19-3ubuntu2.4
- Installed package : gnupg-utils_2.2.19-3ubuntu2
- Fixed package : gnupg-utils_2.2.19-3ubuntu2.4
- Installed package : gpg_2.2.19-3ubuntu2
- Fixed package : gpg_2.2.19-3ubuntu2.4
- Installed package : gpg-agent_2.2.19-3ubuntu2
- Fixed package : gpg-agent_2.2.19-3ubuntu2.4
- Installed package : gpg-wks-client_2.2.19-3ubuntu2
- Fixed package : gpg-wks-client_2.2.19-3ubuntu2.4
- Installed package : gpg-wks-server_2.2.19-3ubuntu2
- Fixed package : gpg-wks-server_2.2.19-3ubuntu2.4
- Installed package : gpgconf_2.2.19-3ubuntu2
- Fixed package : gpgconf_2.2.19-3ubuntu2.4
- Installed package : gpgsm_2.2.19-3ubuntu2
- Fixed package : gpgsm_2.2.19-3ubuntu2.4
- Installed package : gpgv_2.2.19-3ubuntu2
- Fixed package : gpgv_2.2.19-3ubuntu2.4

216590 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Python vulnerability (USN-7280-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7280-1 advisory.

It was discovered that Python incorrectly handled parsing domain names that included square brackets. A remote attacker could possibly use this issue to perform a Server-Side Request Forgery (SSRF) attack.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7280-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

6.3 (CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/V:I:L/V:A:N/SC:N/SI:L/SA:N)

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-2025-0938
XREF USN:7280-1

Plugin Information

Published: 2025/02/21, Modified: 2025/02/21

Plugin Output

tcp/0

```
- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.15

- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.15

- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.15

- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.15

- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.15
```

232304 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerability (USN-7220-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by a vulnerability as referenced in the USN-7220-1 advisory.

It was discovered that Vim incorrectly handled memory when closing buffers with the visual mode active. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7220-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.2 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

3.7 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

3.5 (CVSS2#AV:L/AC:H/Au:S/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

2.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-22134 |
| XREF | USN:7220-1 |
| XREF | IAVA:2025-A-0020-S |

Plugin Information

Published: 2025/03/10, Modified: 2025/03/17

Plugin Output

tcp/0

- Installed package : vim-common_2:8.1.2269-1ubuntu5
- Fixed package : vim-common_2:8.1.2269-1ubuntu5.30
- Installed package : vim-tiny_2:8.1.2269-1ubuntu5
- Fixed package : vim-tiny_2:8.1.2269-1ubuntu5.30
- Installed package : xxd_2:8.1.2269-1ubuntu5
- Fixed package : xxd_2:8.1.2269-1ubuntu5.30

234054 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerabilities (USN-7426-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7426-1 advisory.

It was discovered that poppler incorrectly handled memory when opening certain PDF files. An attacker could possibly use this issue to cause poppler to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7426-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.5 (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)

STIG Severity

I

References

| | |
|------|--------------------|
| CVE | CVE-2025-32364 |
| CVE | CVE-2025-32365 |
| XREF | USN:7426-1 |
| XREF | IAVB:2025-B-0050-S |

Plugin Information

Published: 2025/04/08, Modified: 2025/05/08

Plugin Output

tcp/0

- Installed package : libpoppler-cpp0v5_0.86.1-0ubuntu1
- Fixed package : libpoppler-cpp0v5_0.86.1-0ubuntu1.6
- Installed package : libpoppler-glib8_0.86.1-0ubuntu1
- Fixed package : libpoppler-glib8_0.86.1-0ubuntu1.6
- Installed package : libpoppler97_0.86.1-0ubuntu1
- Fixed package : libpoppler97_0.86.1-0ubuntu1.6
- Installed package : poppler-utils_0.86.1-0ubuntu1
- Fixed package : poppler-utils_0.86.1-0ubuntu1.6

191789 - Ubuntu 20.04 LTS / 22.04 LTS : AccountsService vulnerability (USN-6687-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6687-1 advisory.

It was discovered that AccountsService called a helper incorrectly when performing password change operations. A local attacker could possibly use this issue to obtain encrypted passwords.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6687-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.0 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|---------------|
| CVE | CVE-2012-6655 |
| XREF | USN:6687-1 |

Plugin Information

Published: 2024/03/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : accountsservice_0.6.55-0ubuntu12~20.04.1
- Fixed package : accountsservice_0.6.55-0ubuntu12~20.04.7
- Installed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.1
- Fixed package : gir1.2-accountsservice-1.0_0.6.55-0ubuntu12~20.04.7
- Installed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.1
- Fixed package : libaccountsservice0_0.6.55-0ubuntu12~20.04.7

[214444 - Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerability \(USN-7218-1\)](#)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7218-1 advisory.

It was discovered that Python incorrectly handled parsing bracketed hosts. A remote attacker could possibly use this issue to perform a Server-Side Request Forgery (SSRF) attack.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7218-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v4.0 Base Score

6.3 (CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/V:I:L/V:A:N/SC:N/SI:L/SA:N)

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|------|----------------|
| CVE | CVE-2024-11168 |
| XREF | USN:7218-1 |

Plugin Information

Published: 2025/01/21, Modified: 2025/01/21

Plugin Output

tcp/0

- Installed package : libpython3.8_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8_3.8.10-0ubuntu1~20.04.14
- Installed package : libpython3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-minimal_3.8.10-0ubuntu1~20.04.14
- Installed package : libpython3.8-stdlib_3.8.2-1ubuntu1.2
- Fixed package : libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.14
- Installed package : python3.8_3.8.2-1ubuntu1.2
- Fixed package : python3.8_3.8.10-0ubuntu1~20.04.14
- Installed package : python3.8-minimal_3.8.2-1ubuntu1.2
- Fixed package : python3.8-minimal_3.8.10-0ubuntu1~20.04.14

139692 - Ubuntu 20.04 LTS : GNOME Shell vulnerability (USN-4464-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4464-1 advisory.

It was discovered that GNOME Shell incorrectly handled the login screen password dialog. Sensitive information could possibly be exposed during user logout.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4464-1>

Solution

Update the affected gnome-shell, gnome-shell-common and / or gnome-shell-extension-prefs packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

3.9 (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)

References

| | |
|------|--------------------------------|
| CVE | CVE-2020-17489 |
| XREF | USN:4464-1 |

Plugin Information

Published: 2020/08/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gnome-shell_3.36.3-1ubuntu1~20.04.2
- Fixed package : gnome-shell_3.36.4-1ubuntu1~20.04.2
- Installed package : gnome-shell-common_3.36.3-1ubuntu1~20.04.2
- Fixed package : gnome-shell-common_3.36.4-1ubuntu1~20.04.2

164529 - Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5589-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5589-1 advisory.

Asaf Modelevsky discovered that the Intel(R) 10GbE PCI Express (ixgbe) Ethernet driver for the Linux kernel performed insufficient control flow management. A local attacker could possibly use this to cause a denial of service. (CVE-2021-33061)

It was discovered that the virtual terminal driver in the Linux kernel did not properly handle VGA console font changes, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33656)

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5589-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.9 (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-2021-33061 |
| CVE | CVE-2021-33656 |
| XREF | USN:5589-1 |

Plugin Information

Published: 2022/08/31, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-125-generic for this advisory.

158455 - Ubuntu 20.04 LTS : PolicyKit vulnerability (USN-5304-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5304-1 advisory.

Kevin Backhouse discovered that PolicyKit incorrectly handled file descriptors. A local attacker could possibly use this issue to cause PolicyKit to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5304-1>

Solution

Update the affected 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

5.0 (CVSS:3.0/E:P/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:POC/RL:OF/RC:C)

References

CVE [CVE-2021-4115](#)
XREF USN:5304-1

Plugin Information

Published: 2022/02/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : gir1.2-polkit-1.0_0.105-26ubuntu1
- Fixed package : gir1.2-polkit-1.0_0.105-26ubuntu1.3
- Installed package : libpolkit-agent-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-agent-1-0_0.105-26ubuntu1.3
- Installed package : libpolkit-gobject-1-0_0.105-26ubuntu1
- Fixed package : libpolkit-gobject-1-0_0.105-26ubuntu1.3
- Installed package : policykit-1_0.105-26ubuntu1
- Fixed package : policykit-1_0.105-26ubuntu1.3

141394 - Apache HTTP Server Installed (Linux)

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/08/19

Plugin Output

tcp/0

```
Path : /usr/sbin/apache2
Version : 2.4.41
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS : True
Running : yes

Configs found :
- /etc/apache2/apache2.conf

Loaded modules :
- libphp7.2
- mod_access_compat
- mod_alias
- mod_auth_basic
- mod_authn_core
- mod_authn_file
- mod_authz_core
- mod_authz_host
- mod_authz_user
- mod_autoindex
- mod_deflate
- mod_dir
- mod_env
- mod_filter
- mod_mime
- mod_mpm_prefork
- mod_negotiation
- mod_reqtimeout
- mod_rewrite
- mod_setenvif
- mod_status
```

142640 - Apache HTTP Server Site Enumeration

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/09, Modified: 2025/07/14

Plugin Output

tcp/0

```
Sites and configs present in /usr/sbin/apache2 Apache installation:  
- following sites are present in /etc/apache2/apache2.conf Apache config file:  
+ - *:80  
+ example.com - *:80
```

48204 - Apache HTTP Server Version**Synopsis**

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030
XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://10.22.169.205/  
Version : 2.4.99  
Source : Server: Apache/2.4.41 (Ubuntu)  
backported : 1  
os : ConvertedUbuntu
```

34098 - BIOS Info (SSH)**Synopsis**

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version : 1.2
Vendor : innotek GmbH
Release Date : 12/01/2006
Secure boot : disabled
```

39520 - Backported Security Patch Detection (SSH)**Synopsis**

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

Local checks have been enabled.

39521 - Backported Security Patch Detection (WWW)**Synopsis**

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

Local checks have been enabled.

45590 - Common Platform Enumeration (CPE)**Synopsis**

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:20.04.1:~~lts~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.41 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:exiv2:libexiv2:0.27.2
cpe:/a:gnome:gnome-shell:3.36.3 -> GNOME gnome-shell -
cpe:/a:haxx:libcurl:7.68.0 -> Haxx libcurl
cpe:/a:mariadb:mariadb:10.3.22 -> MariaDB for Node.js
cpe:/a:openbsd:openssh:8.2 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:8.2p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.1.1g -> OpenSSL Project OpenSSL
cpe:/a:openvpn:openvpn:2.4.7 -> OpenVPN
cpe:/a:tukaani:xz:5.2.4 -> Tukaani XZ
cpe:/a:vim:vim:8.1 -> Vim
cpe:/a:vmware:open_vm_tools:11.1.0 -> VMware Open VM Tools
x-cpe:/a:libndp:libndp:1.7

55472 - Device Hostname**Synopsis**

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/07/28

Plugin Output

tcp/0

```
Hostname : ubuntu
ubuntu (hostname command)
```

54615 - Device Type**Synopsis**

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

25203 - Enumerate IPv4 Interfaces via SSH**Synopsis**

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv4 addresses are set on the remote host :

- 10.22.169.205 (on interface enp0s17)
- 127.0.0.1 (on interface lo)

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv6 interfaces are set on the remote host :

- 2409:40c0:106b:64d2:1bf:5adb:5e83:320 (on interface enp0s17)
- fe80::860a:e0ac:e4e3:4edf (on interface enp0s17)
- 2409:40c0:106b:64d2:e68a:b2fc:9941:9ce2 (on interface enp0s17)
- ::1 (on interface lo)

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

The following MAC address exists on the remote host :

- 08:00:27:78:dd:49 (interface enp0s17)

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
lo:  
IPv4:  
- Address : 127.0.0.1  
Netmask : 255.0.0.0  
IPv6:  
- Address : ::1  
Prefixlen : 128  
Scope : host  
ScopeID : 0x10  
enp0s17:  
MAC : 08:00:27:78:dd:49  
IPv4:  
- Address : 10.22.169.205  
Netmask : 255.255.255.0  
Broadcast : 10.22.169.255  
IPv6:  
- Address : 2409:40c0:106b:64d2:1bf:5adb:5e83:320  
Prefixlen : 64  
Scope : global  
ScopeID : 0x0  
- Address : fe80::860a:e0ac:e4e3:4edf  
Prefixlen : 64  
Scope : link  
ScopeID : 0x20  
- Address : 2409:40c0:106b:64d2:e68a:b2fc:9941:9ce2  
Prefixlen : 64  
Scope : global  
ScopeID : 0x0
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:  
enp0s17:  
ipv4_gateways:  
10.22.169.164:  
subnets:  
- 0.0.0.0/0  
ipv6_gateways:  
fe80::4a2:97ff:fec8:6a88:  
subnets:  
- ::/0  
Interface Routes:  
enp0s17:  
ipv4_subnets:  
- 10.22.169.0/24  
- 169.254.0.0/16  
ipv6_subnets:  
- 2409:40c0:106b:64d2::/64  
- fe80::/64
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus has enumerated the path of the current scan user :

```
/usr/local/sbin  
/usr/local/bin  
/usr/sbin  
/usr/bin  
/sbin  
/bin  
/usr/games  
/usr/local/games
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationaly Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>
<http://www.ietf.org/rfc/rfc4941.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

The following card manufacturers were identified :

```
08:00:27:78:DD:49 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

The following is a consolidated list of detected MAC addresses:
- 08:00:27:78:DD:49

168982 - Filepaths contain Dangerous characters (Linux)**Synopsis**

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.

Description

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.

This product has chosen in certain plugins to avoid digging within those files and directories for security reasons.
These should be renamed to avoid security compromise.

Solution

Rename these files or folders to not include dangerous characters.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

The following files and directories contain potentially dangerous characters such as brackets, ampersand, or semicolon.
This scanner avoided access to these files when possible for safety:

liblzma5 5.2.4-1 (via package manager)
xz-utils 5.2.4-1 (via package manager)

43111 - HTTP Methods Allowed (per directory)**Synopsis**

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

<http://www.nessus.org/u?d9c03a9a>
<http://www.nessus.org/u?b019cbdb>
[https://www_OWASP.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www_OWASP.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Apache/2.4.41 (Ubuntu)

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Tue, 04 Nov 2025 09:46:40 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 29 Jul 2020 10:25:45 GMT
ETag: "2aa6-5ab91fa8e8bd0"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Response Body :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016-11-16
See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
```

```
div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.content_section_text {
padding: 4px 8px 4px 8px;

color: #000000;
font-size: 100%;
}

div.content_section_text pre {
margin: 8px 0px 8px 0px;
padding: 8px 8px 8px 8px;

border-width: 1px;
border-style: dotted;
border-color: #000000;

background-color: #F5F6F7;

font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
```

```
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
packaging is derived.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>

<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>
</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
```

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the [manual](/manual) if the apache2-doc package was installed on this server.

```
</p>
<p>
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
</p>
<pre>
/etc/apache2/
|-- apache2.conf
| '-- ports.conf
|-- mods-enabled
| |-- *.load
| '-- *.conf
|-- conf-enabled
| '-- *.conf
|-- sites-enabled
| '-- *.conf
</pre>
<ul>
<li>
<tt>apache2.conf</tt> is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
</li>

<li>
<tt>ports.conf</tt> is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
</li>

<li>
Configuration files in the <tt>mods-enabled</tt>, <tt>conf-enabled</tt> and <tt>sites-enabled</tt> directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
</li>

<li>
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.
</li>

<li>
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>. <b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>

<div class="content_section_text">
<p>
By default, Ubuntu does not allow access through the web browser to <em>any</em> file apart of those located in <tt>/var/www</tt>, <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a> directories (when enabled) and <tt>/usr/share</tt> (for web applications). If your site is using a web document root located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
```

```

Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

Plugin Output

tcp/0

```

+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ enp0s17
+ IPv4
- Address : 10.22.169.205
Assign Method : dynamic
+ IPv6
- Address : 2409:40c0:106b:64d2:1bf:5adb:5e83:320
Assign Method : dynamic
- Address : 2409:40c0:106b:64d2:e68a:b2fc:9941:9ce2
Assign Method : dynamic
- Address : fe80::860a:e0ac:e4e3:4edf
Assign Method : static
```

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.200214' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://github.com/jpirko/libndp>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : libndp0 1.7-0ubuntu1 (via package manager)
Version : 1.7
Managed by OS : True
```

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Dateisystem Größe Benutzt Verf. Verw% Eingehängt auf
udev 1,9G 0 1,9G 0% /dev
tmpfs 394M 2,8M 391M 1% /run
/dev/sda5 20G 8,9G 9,2G 50% /
tmpfs 2,0G 0 2,0G 0% /dev/shm
tmpfs 5,0M 0 5,0M 0% /run/lock
tmpfs 2,0G 0 2,0G 0% /sys/fs/cgroup
/dev/loop0 128K 128K 0 100% /snap/bare/5
/dev/loop3 219M 219M 0 100% /snap/gnome-3-34-1804/93
/dev/loop2 256M 256M 0 100% /snap/gnome-3-34-1804/36
/dev/loop1 56M 56M 0 100% /snap/core18/2959
/dev/loop4 50M 50M 0 100% /snap/snap-store/433
/dev/loop5 50M 50M 0 100% /snap/snap-store/467
/dev/loop7 56M 56M 0 100% /snap/core18/2952
/dev/loop6 92M 92M 0 100% /snap/gtk-common-themes/1535
/dev/loop8 28M 28M 0 100% /snap/snapd/7264
/dev/loop9 30M 30M 0 100% /snap/snapd/8542
/dev/loop10 63M 63M 0 100% /snap/gtk-common-themes/1506
/dev/sda1 511M 4,0K 511M 1% /boot/efi
tmpfs 394M 36K 394M 1% /run/user/125
tmpfs 394M 4,0K 394M 1% /run/user/1000
```

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
```

```

loop0 7:0 0 4K 1 loop /snap/bare/5
loop1 7:1 0 55,5M 1 loop /snap/core18/2959
loop2 7:2 0 255,6M 1 loop /snap/gnome-3-34-1804/36
loop3 7:3 0 218,4M 1 loop /snap/gnome-3-34-1804/93
loop4 7:4 0 49,8M 1 loop /snap/snap-store/433
loop5 7:5 0 49,8M 1 loop /snap/snap-store/467
loop6 7:6 0 91,7M 1 loop /snap/gtk-common-themes/1535
loop7 7:7 0 55,5M 1 loop /snap/core18/2952
loop8 7:8 0 27,1M 1 loop /snap/snapd/7264
loop9 7:9 0 29,9M 1 loop /snap/snapd/8542
loop10 7:10 0 62,1M 1 loop /snap/gtk-common-themes/1506
sda 8:0 0 20G 0 disk
└─sda1 8:1 0 512M 0 part /boot/efi
└─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 19,5G 0 part /

```

\$ mount -l

```

sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=1986948k,nr_inodes=496737,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=403024k,mode=755)
/dev/sda5 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstree on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugegetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugegetlb)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=28,pgrp=1,timeo=0,minproto=5,maxproto=5,direct,pipe_ino=3554)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
hugegetlbfs on /dev/hugepages type hugegetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
traces on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
/var/lib/snapd/snaps/bare_5.snap on /snap/bare/5 type squashfs (ro,nodev,relatime,x-gdu.hide)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
/var/lib/snapd/snaps/gnome-3-34-1804_93.snap on /snap/gnome-3-34-1804/93 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/gnome-3-34-1804_36.snap on /snap/gnome-3-34-1804/36 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/core18_2959.snap on /snap/core18/2959 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/snap-store_433.snap on /snap/snap-store/433 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/snap-store_467.snap on /snap/snap-store/467 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/core18_2952.snap on /snap/core18/2952 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/gtk-common-themes_1535.snap on /snap/gtk-common-themes/1535 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/snapd_7264.snap on /snap/snapd/7264 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/snapd_8542.snap on /snap/snapd/8542 type squashfs (ro,nodev,relatime,x-gdu.hide)
/var/lib/snapd/snaps/gtk-common-themes_1506.snap on /snap/gtk-common-themes/1506 type squashfs (ro,nodev,relatime,x-gdu.hide)
/dev/sda1 on /boot/efi type vfat (rw,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro)
tmpfs on /run/user/125 type tmpfs (rw,nosuid,nodev,relatime,size=403020k,mode=700,uid=125,gid=130)
gvfsd-fuse on /run/user/125/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=125,group_id=130)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=403020k,mode=700,uid=1000,gid=1000)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)

```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: PST -0800
Via timedatectl: Time zone: America/Los_Angeles (PST, -0800)
Via /etc/timezone: America/Los_Angeles
Via /etc/localtime: PST8PDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

-----[User Accounts]-----

```
User : silky
Home folder : /home/silky
Start script : /bin/bash
Groups : lxd
lpadmin
cdrom
silky
sambashare
sudo
plugdev
dip
adm
```

-----[System Accounts]-----

```
User : root
Home folder : /root
Start script : /bin/bash
Groups : root

User : daemon
Home folder : /usr/sbin
Start script : /usr/sbin/nologin
Groups : daemon
```

```
User : bin
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : bin
```

```
User : sys
Home folder : /dev
Start script : /usr/sbin/nologin
Groups : sys
```

```
User : sync
Home folder : /bin
Start script : /bin/sync
Groups : nogroup
```

```
User : games
Home folder : /usr/games
Start script : /usr/sbin/nologin
Groups : games
```

```
User : man
Home folder : /var/cache/man
Start script : /usr/sbin/nologin
Groups : man
```

```
User : lp
Home folder : /var/spool/lpd
```

User : mail
Home folder : /var/mail
Start script : /usr/sbin/nologin
Groups : mail

User : news
Home folder : /var/spool/news
Start script : /usr/sbin/nologin
Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups : uucp

User : proxy
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : proxy

User : www-data
Home folder : /var/www
Start script : /usr/sbin/nologin
Groups : www-data

User : backup
Home folder : /var/backups
Start script : /usr/sbin/nologin
Groups : backup

User : list
Home folder : /var/list
Start script : /usr/sbin/nologin
Groups : list

User : irc
Home folder : /var/run/ircd
Start script : /usr/sbin/nologin
Groups : irc

User : gnats
Home folder : /var/lib/gnats
Start script : /usr/sbin/nologin
Groups : gnats

User : nobody
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : systemd-network
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-network

User : systemd-resolve
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-resolve

User : systemd-timesync
Home folder : /run/systemd
Start script : /usr/sbin/nologin
Groups : systemd-timesync

User : messagebus
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : messagebus

User : syslog
Home folder : /home/syslog
Start script : /usr/sbin/nologin
Groups : syslog
adm

User : _apt
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : tss
Home folder : /var/lib/tpm
Start script : /bin/false
Groups : tss

User : uuidd
Home folder : /run/uuidd
Start script : /usr/sbin/nologin
Groups : uuidd

User : tcpdump
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : tcpdump

User : avahi-autoipd
Home folder : /var/lib/avahi-autoipd
Start script : /usr/sbin/nologin
Groups : avahi-autoipd

User : usbmux
Home folder : /var/lib/usbmux
Start script : /usr/sbin/nologin
Groups : plugdev

User : rtkit
Home folder : /proc
Start script : /usr/sbin/nologin
Groups : rtkit

User : dnsmasq
Home folder : /var/lib/misc
Start script : /usr/sbin/nologin
Groups : nogroup

User : cups-pk-helper
Home folder : /home/cups-pk-helper
Start script : /usr/sbin/nologin
Groups : lpadmin

User : speech-dispatcher
Home folder : /run/speech-dispatcher
Start script : /bin/false
Groups : audio

User : avahi
Home folder : /var/run/avahi-daemon
Start script : /usr/sbin/nologin
Groups : avahi

User : kernoops
Home folder : /
Start script : /usr/sbin/nologin
Groups : nogroup

User : saned
Home folder : /var/lib/saned
Start script : /usr/sbin/nologin
Groups : saned
scanner

User : nm-openvpn
Home folder : /var/lib/openvpn/chroot
Start script : /usr/sbin/nologin
Groups : nm-openvpn

User : hplip
Home folder : /run/hplip
Start script : /bin/false
Groups : lp

User : whoopsie
Home folder : /nonexistent
Start script : /bin/false
Groups : whoopsie

User : colord
Home folder : /var/lib/colord
Start script : /usr/sbin/nologin
Groups : colord

User : geoclue
Home folder : /var/lib/geoclue
Start script : /usr/sbin/nologin
Groups : geoclue

User : pulse
Home folder : /var/run/pulse
Start script : /usr/sbin/nologin
Groups : pulse
audio

User : gnome-initial-setup
Home folder : /run/gnome-initial-setup/
Start script : /bin/false
Groups : nogroup

User : gdm
Home folder : /var/lib/gdm3
Start script : /bin/false
Groups : gdm

User : systemd-coredump
Home folder : /
Start script : /usr/sbin/nologin
Groups : systemd-coredump

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql

User : sshd
Home folder : /run/sshd

```
Start script : /usr/sbin/nologin
Groups : nogroup
```

```
-----[ Domain Accounts ]-----
```

130626 - MariaDB Client/Server Installed (Linux)

Synopsis

One or more MariaDB server or client versions are available on the remote Linux host.

Description

One or more MariaDB server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/08, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path : mariadb-client-10.3 (via package manager)
Version : 10.3.22
Managed : 1
Product : MariaDB Client
```

tcp/0

```
Path : mariadb-server-10.3 (via package manager)
Version : 10.3.22
Managed : 1
Product : MariaDB Server
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

The following password policy is defined on the remote host:

```
Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
```

Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

<http://technet.microsoft.com/en-us/library/bb418944.aspx>

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

The remote host SID value is : S-1-5-21-4134020711-1526993497-85718105

The value of 'RestrictAnonymous' setting is : unknown

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

Nessus was able to obtain the following information about the host, by parsing the SMB2 Protocol's NTLM SSP message:

Target Name: UBUNTU
NetBIOS Domain Name: UBUNTU
NetBIOS Computer Name: UBUNTU
DNS Domain Name:

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

An SMB server is running on this port.

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

A CIFS server is running on this port.

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

<https://technet.microsoft.com/en-us/library/bb456988.aspx>
<https://technet.microsoft.com/en-us/library/cc783530.aspx>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

Plugin Output

tcp/445/cifs

```

Share path : \\UBUNTU\print$  

Local path : C:\var\lib\samba\printers  

Comment : Printer Drivers  

[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff  

FILE_GENERIC_READ: YES  

FILE_GENERIC_WRITE: YES  

FILE_GENERIC_EXECUTE: YES

Share path : \\UBUNTU\Notes  

Local path : C:\home\silky\Note  

Comment : My Notes  

[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff  

FILE_GENERIC_READ: YES  

FILE_GENERIC_WRITE: YES  

FILE_GENERIC_EXECUTE: YES

Share path : \\UBUNTU\IPC$  

Local path : C:\tmp  

Comment : IPC Service (ubuntu server (Samba, Ubuntu))  

[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff  

FILE_GENERIC_READ: YES  

FILE_GENERIC_WRITE: YES  

FILE_GENERIC_EXECUTE: YES

```

10395 - Microsoft Windows SMB Shares Enumeration**Synopsis**

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

Here are the SMB shares available on the remote host :

- print\$
- Notes
- IPC\$

100871 - Microsoft Windows SMB Versions Supported (remote check)**Synopsis**

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

The remote host supports the following versions of SMB :
SMBv2

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

The remote host supports the following SMB dialects :
version _introduced in windows version_
2.0.2 Windows 2008
2.1 Windows 7
2.2.2 Windows 8 Beta
2.2.4 Windows 8 Beta
3.0 Windows 8
3.0.2 Windows 8.1
3.1 Windows 10
3.1.1 Windows 10

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialled or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus
```

```
ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.
```

```
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Tiki
Scan policy used : Advanced Scan
Scanner IP : 10.22.169.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 159.078 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialated checks : yes, as 'silky' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/11/4 9:46 UTC
Scan duration : 398 sec
Scan for malware : no
```

64582 - Netstat Connection Information**Synopsis**

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)**Synopsis**

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

Port 22/tcp was found to be open

14272 - Netstat Portscanner (SSH)**Synopsis**

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/137/netbios-ns

Port 137/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/138

Port 138/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/139/smb

Port 139/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/445/cifs

Port 445/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/631

Port 631/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5353/mdns

Port 5353/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/44793

Port 44793/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/48441

Port 48441/udp was found to be open

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Ubuntu 18.04 Linux Kernel 4.15

Confidence level : 56

Method : MLSinFP

Type : unknown

Fingerprint : unknown

Remote operating system : Linux Kernel 5.4.0-42-generic

Confidence level : 99

Method : uname

Type : general-purpose

Fingerprint : uname:Linux ubuntu 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

Remote operating system : Linux Kernel 2.6

Confidence level : 65

Method : SinFP

Type : general-purpose

Fingerprint : SinFP:

P1:B10113:F0x12:W64240:00204fffff:M1460:

P2:B10113:F0x12:W65160:00204fffff0402080afffffff4445414401030307:M1460:

P3:B00000:F0x00:W0:00:M0

P4:191303_7_p=139

Remote operating system : Linux Kernel 5.4.0-42-generic on Ubuntu 20.04

Confidence level : 100

Method : LinuxDistribution

Type : general-purpose

Fingerprint : unknown

Following fingerprints could not be used to determine OS :

SSH:!SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1

HTTP:!Server: Apache/2.4.41 (Ubuntu)

11936 - OS Identification**Synopsis**

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

Remote operating system : Linux Kernel 5.4.0-42-generic on Ubuntu 20.04

Confidence level : 100

Method : LinuxDistribution

The remote host is running Linux Kernel 5.4.0-42-generic on Ubuntu 20.04

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)**Synopsis**

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :

Linux ubuntu 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.

The remote Debian system is :

bullseye/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.

Runtime : 4.941108 seconds

117887 - OS Security Patch Assessment Available**Synopsis**

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

OS Security Patch Assessment is available.

Account : silky

Protocol : SSH

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.2p1
Banner : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

168007 - OpenSSL Installed (Linux)**Synopsis**

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : openssl 1.1.1g-1 (via package manager)
Version : 1.1.1g
Managed by OS : True
```

232856 - OpenVPN Installed (Linux)

Synopsis

OpenVPN is installed on the remote Linux host.

Description

OpenVPN is installed on the remote Linux host.

Note: Enabling the 'Perform thorough tests' setting will search the file system more broadly.

See Also

<https://openvpn.net/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/19, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : openvpn 2.4.7-1ubuntu2 (via package manager)
Version : 2.4.7
Managed by OS : True
```

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

. You need to take the following 604 actions :

[SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315)]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1) (200307)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1) (201111)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1) (194474)]

+ Action to take : Update the affected less package.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerability (USN-6744-1) (193701)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities (USN-6891-1) (202187)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 41 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1) (192219)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server vulnerabilities (USN-6721-1) (192938)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1) (193362)]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1) (190598)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Requests vulnerabilities (USN-7568-1) (240162)]

+ Action to take : Update the affected python-requests, python-requests-whl and / or python3-requests packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Setuptools vulnerability (USN-7544-1) (237449)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Expat vulnerability (USN-7145-1) (212213)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerability (USN-7257-1) (214997)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerabilities (USN-7419-1) (233967)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerability (USN-7542-1) (237448)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Setuptools vulnerability (USN-7002-1) (207058)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerabilities (USN-6993-1) (206625)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : libarchive vulnerabilities (USN-7070-1) (209121)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : rsync vulnerabilities (USN-7206-1) (214143)]

+ Action to take : Update the affected rsync package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : wpa_supplicant and hostapd vulnerability (USN-6945-1) (205112)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libxslt vulnerability (USN-7600-1) (241065)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 : LibTIFF vulnerabilities (USN-6644-1) (190713)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 24.04 LTS : Expat vulnerabilities (USN-7000-1) (207059)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-7679-1) (243224)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 20.04 LTS : Python vulnerabilities (USN-7348-1) (232662)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libsndfile vulnerabilities (USN-7273-1) (216423)]

+ Action to take : Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS : Libcroco vulnerabilities (USN-6958-1) (205444)]

+ Action to take : Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Avahi vulnerabilities (USN-6487-1) (186016)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : BlueZ vulnerability (USN-6540-1) (186644)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1) (186711)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Intel Microcode vulnerability (USN-6485-1) (185930)]

+ Action to take : Update the affected intel-microcode package.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6557-1) (186991)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 27 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libsndfile vulnerability (USN-6471-1) (184303)]

+ Action to take : Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : procps-ng vulnerability (USN-6477-1) (185569)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : urllib3 vulnerabilities (USN-6473-1) (185342)]

+ Action to take : Update the affected python-urllib3 and / or python3-urllib3 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : AMD Microcode vulnerability (USN-6319-1) (180268)]

+ Action to take : Update the affected amd64-microcode package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1) (186676)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Ghostscript vulnerability (USN-6297-1) (179940)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Intel Microcode vulnerabilities (USN-6286-1) (179733)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerability (USN-6428-1) (182891)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6257-1) (178940)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6139-1) (176714)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Vim vulnerabilities (USN-6154-1) (177108)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 : Ceph vulnerability (USN-6613-1) (189748)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-6512-1) (186225)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6270-1) (179306)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : gawk vulnerability (USN-6373-1) (181451)]

+ Action to take : Update the affected gawk package.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : poppler vulnerabilities (USN-6508-1) (186209)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : Ghostscript vulnerabilities (USN-6364-1) (181362)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : elfutils vulnerabilities (USN-6322-1) (180321)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : nghttp2 vulnerability (USN-6142-1) (176745)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : poppler vulnerabilities (USN-6299-1) (179941)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : GNU binutils vulnerabilities (USN-6101-1) (176325)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ncurses vulnerabilities (USN-6099-1) (176244)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : snapd vulnerability (USN-6125-1) (176501)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5487-1) (162425)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : DBus vulnerabilities (USN-5704-1) (166619)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Dnsmasq vulnerability (USN-6034-1) (174553)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerability (USN-5638-3) (168153)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : FLAC vulnerabilities (USN-5733-1) (168010)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU binutils vulnerability (USN-5762-1) (168452)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerability (USN-6017-1) (174272)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerabilities (USN-5886-1) (171928)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : JBIG-KIT vulnerability (USN-5742-1) (168193)]

+ Action to take : Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Kerberos vulnerabilities (USN-5828-1) (170651)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5923-1) (172213)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 31 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5688-1) (166264)]

+ Action to take : Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5996-1) (173861)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5485-1) (162394)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Mako vulnerability (USN-5625-1) (165282)]

+ Action to take : Update the affected python-mako and / or python3-mako packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM regressions (USN-5825-2) (171011)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Perl vulnerability (USN-5689-1) (166266)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-5960-1) (172632)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Setuptools vulnerability (USN-5817-1) (170412)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5963-1) (173039)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerabilities (USN-5740-1) (168152)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : apr-util vulnerability (USN-5870-1) (171484)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerability (USN-5587-1) (164627)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : e2fsprogs vulnerability (USN-5464-1) (161938)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : poppler vulnerability (USN-5606-1) (164950)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : python-future vulnerability (USN-5833-1) (170898)]

+ Action to take : Update the affected python-future and / or python3-future packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : shadow vulnerability (USN-5745-1) (168227)]

+ Action to take : Update the affected login, passwd and / or uidmap packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : snapd vulnerability (USN-5753-1) (168316)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : systemd vulnerabilities (USN-5928-1) (172227)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : tar vulnerability (USN-5900-1) (172025)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : unzip vulnerabilities (USN-5673-1) (166103)]

+ Action to take : Update the affected unzip package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Aspell vulnerability (USN-5023-1) (152079)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1) (159982)]

+ Action to take : Update the affected bash, bash-builtins and / or bash-static packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : BlueZ vulnerability (USN-5275-1) (157457)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-5043-1) (152637)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Expat vulnerabilities and regression (USN-5320-1) (158789)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GMP vulnerability (USN-5672-1) (166088)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GNOME grilo vulnerability (USN-5055-1) (152917)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Base Plugins vulnerability (USN-4959-1) (149650)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-5555-1) (163923)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5849-1) (171212)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4985-1) (150394)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5421-1) (161209)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1) (170011)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5493-1) (162552)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) (174907)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-5342-1) (159255)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Speex vulnerability (USN-5280-1) (157882)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5147-1) (155351)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1) (159882)]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libcaca vulnerabilities (USN-5119-1) (154328)]

+ Action to take : Update the affected caca-utils, libcaca-dev and / or libcaca0 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libsepol vulnerabilities (USN-5391-1) (160233)]

+ Action to take : Update the affected libsepoll, libsepoll-dev and / or sepol-utils packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5573-1) (164287)]

+ Action to take : Update the affected rsync package.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : tar vulnerability (USN-5329-1) (158932)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : CUPS vulnerability (USN-6844-1) (200879)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GDK-PixBuf vulnerability (USN-6806-1) (200128)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1) (198244)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1) (198069)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1) (197569)]

+ Action to take : Update the affected pypy-idna, python-idna and / or python3-idna packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : GIFLIB vulnerabilities (USN-6824-1) (200257)]

+ Action to take : Update the affected giflib-tools, libgif-dev and / or libgif7 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1) (191066)]

+ Action to take : Update the affected less package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1) (193905)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Apport vulnerability (USN-7545-1) (237709)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Ghostscript vulnerabilities (USN-7623-1) (241623)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Intel Microcode vulnerabilities (USN-7535-1) (237338)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : LibRaw vulnerabilities (USN-7485-1) (235341)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libsoup vulnerabilities (USN-7543-1) (237450)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libvpx vulnerability (USN-7551-1) (237727)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : urllib3 vulnerabilities (USN-7599-1) (240700)]

+ Action to take : Update the affected python-urllib3 and / or python3-urllib3 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : AMD Microcode vulnerability (USN-7077-1) (209342)]

+ Action to take : Update the affected amd64-microcode package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7149-1) (212270)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenJPEG vulnerabilities (USN-7223-1) (214505)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerability (USN-7213-1) (214326)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : urllib3 vulnerability (USN-7084-1) (209876)]

+ Action to take : Update the affected python-urllib3 and / or python3-urllib3 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : GDK-PixBuf vulnerabilities (USN-7662-1) (242586)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : libsoup vulnerabilities (USN-7643-1) (242278)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : APR vulnerability (USN-7038-1) (207799)]

+ Action to take : Update the affected libapr1, libapr1-dev and / or libapr1t64 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : GLib vulnerability (USN-7114-1) (211522)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Intel Microcode vulnerabilities (USN-7033-1) (207723)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : LibTIFF vulnerability (USN-6997-1) (206788)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJPEG vulnerability (USN-7037-1) (207801)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerability (USN-7048-1) (207996)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : nano vulnerability (USN-7064-1) (209028)]

+ Action to take : Update the affected nano and / or nano-tiny packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7269-1) (216387)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-6809-1) (200132)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : gdb vulnerabilities (USN-6842-1) (200771)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : APT vulnerability (USN-4667-1) (144013)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : AccountsService vulnerabilities (USN-4616-1) (142371)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-4458-1) (139596)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4449-1) (139369)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4720-1) (146068)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Aptdaemon vulnerabilities (USN-4664-1) (143584)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4468-1) (139770)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4929-1) (149092)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Brotli vulnerability (USN-4568-1) (141179)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Dnsmasq vulnerabilities (USN-4698-1) (145078)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : File Roller vulnerability (USN-4927-1) (148987)]

+ Action to take : Update the affected file-roller package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4474-1) (139908)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4926-1) (148992)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 60 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : FreeType vulnerability (USN-4593-1) (141615)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GLib vulnerability (USN-4764-1) (147989)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GRUB 2 vulnerabilities (USN-4432-1) (139179)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-4928-1) (149055)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-4469-1) (139782)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 26 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-1) (142731)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Kerberos vulnerability (USN-4635-1) (142967)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-4755-1) (148000)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer, Vino vulnerability (USN-4636-1) (142998)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4591-1) (141541)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4489-1) (140450)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4627-1) (142721)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4694-1) (145007)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4716-1) (146044)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 73 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-4476-1) (140030)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Net-SNMP vulnerabilities (USN-4471-1) (139784)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Nettle vulnerability (USN-4906-1) (148491)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4744-1) (147986)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PEAR vulnerability (USN-4723-1) (146301)]

+ Action to take : Update the affected php-pear package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PackageKit vulnerabilities (USN-4538-1) (183597)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Perl vulnerabilities (USN-4602-1) (141913)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-4763-1) (147998)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PulseAudio vulnerability (USN-4640-1) (143214)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pygments vulnerability (USN-4897-1) (148248)]

+ Action to take : Update the affected python-pygments and / or python3-pygments packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-4754-1) (147997)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Raptor vulnerability (USN-4630-1) (142739)]

+ Action to take : Update the affected libraptor2-0, libraptor2-dev and / or raptor2-utils packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4454-1) (139479)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4930-1) (149093)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Software Properties vulnerability (USN-4457-1) (139568)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Sudo vulnerabilities (USN-4705-1) (145463)]

+ Action to take : Update the affected sudo and / or sudo-ldap packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Vino vulnerabilities (USN-4573-1) (141301)]

+ Action to take : Update the affected vino package.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Whoopsie vulnerabilities (USN-4450-1) (139370)]

+ Action to take : Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4490-1) (140451)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4905-1) (148495)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-4898-1) (148260)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerability (USN-4466-1) (139724)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ldb vulnerabilities (USN-4888-1) (148089)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libcaca vulnerability (USN-4921-1) (148856)]

+ Action to take : Update the affected caca-utils, libcaca-dev and / or libcaca0 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif vulnerability (USN-4624-1) (142732)]

+ Action to take : Update the affected libexif-dev and / or libexif12 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libfcgi-perl vulnerability (USN-7527-1) (237111)]

+ Action to take : Update the affected libfcgi-perl package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libproxy vulnerability (USN-4673-1) (144704)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libssh vulnerability (USN-4447-1) (139367)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libx11 vulnerabilities (USN-4487-1) (140266)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : p11-kit vulnerabilities (USN-4677-1) (144747)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ppp vulnerability (USN-4451-1) (139371)]

+ Action to take : Update the affected ppp, ppp-dev and / or ppp-udeb packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-apt vulnerability (USN-4668-1) (144015)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-cryptography vulnerability (USN-4613-1) (142368)]

+ Action to take : Update the affected python-cryptography and / or python3-cryptography packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : sane-backends vulnerabilities (USN-4470-1) (139783)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : snapd vulnerability (USN-4728-1) (146351)]

+ Action to take : Update the affected packages.

```
[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : tar vulnerabilities (USN-4692-1) (144944) ]
+ Action to take : Update the affected tar and / or tar-scripts packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : urllib3 vulnerability (USN-4570-1) (141177) ]
+ Action to take : Update the affected python-urllib3 and / or python3-urllib3 packages.

[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4757-1) (147984) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils vulnerability (USN-4649-1) (143268) ]
+ Action to take : Update the affected xdg-utils package.

[ Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : FreeRDP vulnerabilities (USN-6401-1) (182520) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) (178653) ]
+ Action to take : Update the affected kernel package.

[ Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6420-1) (182769) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 28 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) (178914) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6284-1) (179704) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6317-1) (180257) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6340-1) (180512) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6387-1) (181641) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6417-1) (182578) ]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[ Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6441-1) (183455) ]
```

+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6462-1) (184085)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-1) (186082)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6548-1) (186743)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6605-1) (189614)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6625-1) (190124)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6128-1) (176550)]
+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities (USN-6060-1) (175283)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : TeX Live vulnerability (USN-6115-1) (176478)]
+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6075-1) (175722)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : cups-filters vulnerability (USN-6083-1) (175977)]
+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6078-1) (175916)]
+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : eSpeak NG vulnerabilities (USN-6858-1) (201188)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : python-cryptography vulnerabilities (USN-6673-1) (191499)]
+ Action to take : Update the affected python-cryptography and / or python3-cryptography packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Python vulnerabilities (USN-7570-1) (240097)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : poppler vulnerabilities (USN-7471-1) (234994)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU C Library vulnerability (USN-7259-1) (215062)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7126-1) (211896)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5942-1) (172444)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apport vulnerability (USN-6018-1) (174274)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Bind vulnerabilities (USN-5626-1) (165290)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : CUPS vulnerabilities (USN-5454-1) (161723)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ceph vulnerabilities (USN-6063-1) (175537)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : DHCP vulnerabilities (USN-5658-1) (165706)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Exempi vulnerabilities (USN-5483-1) (162376)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerabilities (USN-5638-2) (167852)]

+ Action to take : Update the affected expat, libexpat1 and / or libexpat1-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeRDP vulnerabilities (USN-5734-1) (168146)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeType vulnerabilities (USN-5528-1) (163305)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNOME Files vulnerability (USN-5786-1) (169587)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU C Library vulnerability (USN-7541-1) (237431)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerabilities (USN-5643-1) (165504)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuPG vulnerability (USN-5503-1) (162734)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuTLS vulnerabilities (USN-5550-1) (163872)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : HTTP-Daemon vulnerability (USN-5520-1) (163106)]

+ Action to take : Update the affected libhttp-daemon-perl package.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerability (USN-5612-1) (165109)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerability (USN-5743-2) (168337)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5787-1) (169583)]

+ Action to take : Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5476-1) (162172)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibreOffice vulnerabilities (USN-5694-1) (166339)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libxslt vulnerabilities (USN-5575-1) (164327)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5823-1) (170565)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 77 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NSS vulnerabilities (USN-5892-1) (171951)]

+ Action to take : Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NTFS-3G vulnerability (USN-5711-1) (166861)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Net-SNMP vulnerabilities (USN-5795-1) (169711)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Open VM Tools vulnerability (USN-5578-1) (164376)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-5424-1) (161250)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Protocol Buffers vulnerabilities (USN-5945-1) (172495)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : PyJWT vulnerability (USN-5526-1) (163294)]

+ Action to take : Update the affected python-jwt and / or python3-jwt packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-5767-1) (168516)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Rsyslog vulnerability (USN-5404-1) (160674)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : SQLite vulnerability (USN-5716-1) (167061)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Sudo vulnerabilities (USN-6005-1) (174161)]

+ Action to take : Update the affected sudo and / or sudo-ldap packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-6015-1) (174266)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 109 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6026-1) (174460)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 59 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Wayland vulnerability (USN-5614-1) (165205)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerability (USN-5986-1) (173648)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5964-1) (173037)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 25 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : dpkg vulnerability (USN-5446-1) (161613)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : libXpm vulnerabilities (USN-5807-1) (170110)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : networkd-dispatcher vulnerabilities (USN-5395-1) (160308)]

+ Action to take : Update the affected networkd-dispatcher package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : pixman vulnerability (USN-5718-1) (167196)]

+ Action to take : Update the affected libpixman-1-0 and / or libpixman-1-dev packages.

[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : rsync vulnerabilities (USN-5921-1) (172126)]

+ Action to take : Update the affected rsync package.

[Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-5333-1) (159024)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-5077-1) (153367)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Avahi vulnerabilities (USN-5008-1) (151452)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-5332-1) (159059)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : BlueZ vulnerabilities (USN-5155-1) (155687)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : BusyBox vulnerabilities (USN-5179-1) (155939)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Cyrus SASL vulnerability (USN-5301-1) (158259)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : DBus vulnerability (USN-5244-2) (160853)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : DHCP vulnerability (USN-4969-1) (150030)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : DjVuLibre vulnerabilities (USN-4957-1) (149527)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Dnsmasq vulnerability (USN-4976-1) (150143)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-6074-1) (175671)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 262 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-4481-1) (140179)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-5154-1) (155681)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : FriBidi vulnerabilities (USN-5366-1) (159589)]

+ Action to take : Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : GDM vulnerability (USN-4614-1) (142369)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar vulnerability (USN-4937-1) (149332)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : GNU C Library vulnerabilities (USN-5310-1) (158502)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : GNU binutils vulnerabilities (USN-5124-1) (154413)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : GNU cpio vulnerability (USN-5064-1) (153143)]

+ Action to take : Update the affected cpio and / or cpio-win32 packages.

[Ubuntu 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-5224-1) (156645)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Gzip vulnerability (USN-5378-1) (159711)]

+ Action to take : Update the affected gzip and / or gzip-win32 packages.

[Ubuntu 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-3) (149521)]

+ Action to take : Update the affected intel-microcode package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Kerberos vulnerabilities (USN-5959-1) (172631)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : LZ4 vulnerability (USN-4968-1) (149988)]
+ Action to take : Update the affected packages.
[Ubuntu 18.04 LTS / 20.04 LTS : LibRaw vulnerabilities (USN-5715-1) (167060)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5523-2) (164944)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Libgcrypt vulnerabilities (USN-5080-1) (153447)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : LibreOffice vulnerability (USN-6023-1) (174410)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel update (USN-4689-4) (145234)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4483-1) (140181)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4525-1) (140723)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4576-1) (141451)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4658-1) (143431)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4679-1) (144750)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4689-2) (144869)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4750-1) (148009) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4878-1) (148003) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4887-1) (148034) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4909-1) (148497) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4917-1) (148690) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4945-1) (149416) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4982-1) (150233) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5000-1) (150957) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5017-1) (153129) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5045-1) (152639) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5071-1) (153178) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5091-1) (153769) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).
```

```
[ Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5116-1) (154278) ]
```

+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5137-1) (154980)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5163-1) (155749)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5210-1) (156481)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5267-1) (157353)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5318-1) (158737)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5338-1) (159144)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5358-1) (159373)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5384-1) (160025)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5415-1) (161063)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5442-1) (161810)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5467-1) (161950)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5514-1) (163113)]
+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5562-1) (164036)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5622-1) (165287)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5668-1) (166012)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5691-1) (166286)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5728-1) (167771)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5756-1) (168348)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1) (169689)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1) (171261)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1) (172135)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) (174461)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1) (176228)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) (176564)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6648-1) (190874)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6681-1) (191663)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6702-1) (192292)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6726-1) (193081)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 23 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6741-1) (193596)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6767-1) (195135)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 48 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6776-1) (197218)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6831-1) (200450)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 42 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6868-1) (201871)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6896-1) (202292)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 149 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6924-1) (204835)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1) (205223)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 83 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6973-1) (206077)]

+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7022-1) (207398)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7073-1) (209164)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7088-1) (210006)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 162 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7159-1) (212722)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 23 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7173-1) (213100)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7234-1) (214732)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7293-1) (216774)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 145 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7391-1) (233669)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 153 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7408-1) (233783)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7461-1) (234814)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7495-1) (235357)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7516-1) (236878)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 90 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7585-1) (240211)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 32 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7671-1) (242901)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5240-1) (156879)]

+ Action to take : Update the affected kernel package.

[Ubuntu 18.04 LTS / 20.04 LTS : MariaDB vulnerabilities (USN-4603-1) (141921)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-5270-1) (157356)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 133 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-5410-1) (161025)]

+ Action to take : Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Nettle vulnerabilities (USN-4990-1) (150857)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : OpenVPN vulnerability (USN-5347-1) (159204)]

+ Action to take : Update the affected openvpn package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : PEAR vulnerability (USN-5027-1) (152143)]

+ Action to take : Update the affected php-pear package.

[Ubuntu 18.04 LTS / 20.04 LTS : Paramiko vulnerability (USN-5351-1) (159331)]

+ Action to take : Update the affected python-paramiko and / or python3-paramiko packages.

[Ubuntu 18.04 LTS / 20.04 LTS : Perl DBI module vulnerabilities (USN-5030-1) (152230)]

+ Action to take : Update the affected libdbi-perl package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Pillow vulnerability (USN-5227-3) (166448)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : PolicyKit vulnerability (USN-5252-1) (157112)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : QPDF vulnerabilities (USN-5026-1) (152145)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : SPICE vdagent vulnerabilities (USN-4617-1) (142464)]

+ Action to take : Update the affected spice-vdagent package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-5615-1) (165204)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Squashfs-Tools vulnerability (USN-5078-1) (153391)]

+ Action to take : Update the affected squashfs-tools package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5393-1) (160275)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 77 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5247-1) (157143)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : WavPack vulnerability (USN-4682-1) (144789)]

+ Action to take : Update the affected libwavpack-dev, libwavpack1 and / or wavpack packages.

[Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4444-1) (139311)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-5087-1) (153568)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 30 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : X.Org X Server vulnerabilities (USN-5193-1) (156076)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : XZ Utils vulnerability (USN-5378-2) (159714)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-5079-1) (153407)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : libinput vulnerability (USN-5382-1) (160028)]

+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : libjpeg-turbo vulnerabilities (USN-5631-1) (165321)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : libsndfile vulnerability (USN-5025-1) (152136)]
+ Action to take : Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

[Ubuntu 18.04 LTS / 20.04 LTS : libwebp vulnerabilities (USN-4971-1) (150131)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : libx11 vulnerability (USN-4966-1) (149903)]
+ Action to take : Update the affected packages.

[Ubuntu 18.04 LTS / 20.04 LTS : libzstd vulnerabilities (USN-4760-1) (148007)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5359-1) (159380)]
+ Action to take : Update the affected rsync package.

[Ubuntu 18.04 LTS / 20.04 LTS : snapd vulnerabilities (USN-5292-1) (158135)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : systemd vulnerabilities (USN-5013-1) (151836)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : tcpdump vulnerabilities (USN-5331-2) (159631)]
+ Action to take : Update the affected tcpdump package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 18.04 LTS / 20.04 LTS : zlib vulnerability (USN-5355-1) (159363)]
+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 : curl vulnerabilities (USN-6237-1) (178481)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Apache HTTP Server vulnerabilities (USN-6506-1) (186191)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : FreeRDP vulnerabilities (USN-6522-1) (186445)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNOME Settings vulnerability (USN-6554-1) (186809)]
+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Ghostscript vulnerability (USN-6433-1) (183231)]
+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerabilities (USN-6593-1) (189294)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : MySQL vulnerabilities (USN-6459-1) (184027)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Open VM Tools vulnerabilities (USN-6463-1) (184088)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6565-1) (187627)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : PAM vulnerability (USN-6588-1) (189143)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Perl vulnerabilities (USN-6517-1) (186300)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : SQLite vulnerabilities (USN-6566-1) (187626)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6563-1) (187429)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 24 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6587-1) (189087)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : curl vulnerabilities (USN-6535-1) (186615)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerabilities (USN-6592-1) (189295)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : nghttp2 vulnerability (USN-6505-1) (186192)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : python-cryptography vulnerabilities (USN-6539-1) (186623)]

+ Action to take : Update the affected python-cryptography and / or python3-cryptography packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : AccountsService vulnerability (USN-6190-1) (177711)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Avahi vulnerability (USN-6129-1) (176562)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Bind vulnerabilities (USN-6390-1) (181689)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUE vulnerability (USN-6423-1) (182791)]

+ Action to take : Update the affected libcue-dev and / or libcue2 packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6391-1) (181687)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : GStreamer Base Plugins vulnerabilities (USN-6268-1) (179246)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : GStreamer Good Plugins vulnerability (USN-6269-1) (179247)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Ghostscript vulnerability (USN-6213-1) (178108)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Kerberos vulnerability (USN-6467-2) (184451)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : LibRaw vulnerabilities (USN-6137-1) (176715)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities (USN-6288-1) (179881)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6365-1) (181363)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : OpenSSH vulnerability (USN-6242-1) (178755)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Perl vulnerability (USN-6112-2) (176670)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6513-2) (186307)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : ReportLab vulnerability (USN-6196-1) (177902)]

+ Action to take : Update the affected python3-renderpm, python3-reportlab and / or python3-reportlab-accel packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Requests vulnerability (USN-6155-1) (177111)]

+ Action to take : Update the affected python3-requests package.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Samba vulnerabilities (USN-6425-1) (182845)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6405-1) (182432)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 33 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : WebKitGTK vulnerabilities (USN-6061-1) (175285)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : YAJL vulnerabilities (USN-6233-2) (186986)]

+ Action to take : Update the affected libyajl-dev, libyajl2 and / or yajl-tools packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : curl vulnerabilities (USN-6429-1) (182907)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libXpm vulnerabilities (USN-6408-1) (182470)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libcap2 vulnerabilities (USN-6166-1) (177325)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : librsvg vulnerability (USN-6266-1) (179146)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libssh vulnerabilities (USN-6138-1) (176712)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libvpx vulnerabilities (USN-6403-1) (182421)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6369-1) (181426)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libx11 vulnerabilities (USN-6407-1) (182471)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : poppler vulnerabilities (USN-6273-1) (179334)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-1) (201972)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

```
[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1) (195216) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GStreamer Base Plugins vulnerability (USN-6798-1) (198070) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Ghostscript vulnerabilities (USN-6835-1) (200676) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibreOffice vulnerability (USN-6789-1) (198045) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : MySQL vulnerabilities (USN-6823-1) (200259) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Netplan vulnerabilities (USN-6851-1) (201048) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : OpenVPN vulnerabilities (USN-6860-1) (201237) ]
+ Action to take : Update the affected openvpn package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1) (198063) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : VTE vulnerability (USN-6833-1) (200488) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Wget vulnerability (USN-6852-1) (201043) ]
+ Action to take : Update the affected wget package.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libndp vulnerability (USN-6830-1) (200438) ]
+ Action to take : Update the affected libndp-dev, libndp-tools and / or libndp0 packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libvpx vulnerability (USN-6814-1) (200175) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache HTTP Server vulnerabilities (USN-6729-1) (193232) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Dnsmasq vulnerabilities (USN-6657-1) (191021) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : FreeRDP vulnerabilities (USN-6752-1) (193891) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1) (193515) ]
```

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1) (194475)]

+ Action to take : Update the affected cpio and / or cpio-win32 packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1) (193341)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MariaDB vulnerabilities (USN-6600-1) (189536)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MySQL vulnerabilities (USN-6615-1) (189776)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1) (193171)]

+ Action to take : Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Paramiko vulnerability (USN-6598-1) (189519)]

+ Action to take : Update the affected python3-paramiko package.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerabilities (USN-6618-1) (189830)]

+ Action to take : Update the affected python3-pil and / or python3-pil.imagetk packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : TeX Live vulnerabilities (USN-6695-1) (192119)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6840-1) (200724)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 47 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1) (192621)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libuv vulnerability (USN-6666-1) (191103)]

+ Action to take : Update the affected libuv1 and / or libuv1-dev packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2) (193159)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : GLib vulnerability (USN-7532-1) (237250)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : MySQL vulnerabilities (USN-7479-1) (235159)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 27 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Open VM Tools vulnerability (USN-7508-1) (235829)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : OpenSSH vulnerability (USN-7457-1) (234810)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : SQLite vulnerabilities (USN-7528-1) (237145)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Yelp vulnerability (USN-7447-1) (234777)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libarchive vulnerabilities (USN-7454-1) (234800)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : net-tools vulnerability (USN-7537-1) (237384)]

+ Action to take : Update the affected net-tools package.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : systemd vulnerability (USN-7559-1) (238067)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Bind vulnerabilities (USN-7241-1) (214790)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU binutils vulnerabilities (USN-7423-1) (233981)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Base Plugins vulnerabilities (USN-7175-1) (213188)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Good Plugins vulnerabilities (USN-7176-1) (213187)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer vulnerability (USN-7174-1) (213189)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Ghostscript vulnerabilities (USN-7378-1) (233470)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GnuPG vulnerability (USN-7412-1) (233821)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GnuTLS vulnerability (USN-7281-1) (216587)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerabilities (USN-7314-1) (217107)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerability (USN-7504-1) (235613)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Libxslt vulnerability (USN-7361-1) (233046)]

+ Action to take : Update the affected libxslt1-dev, libxslt1.1 and / or xsltproc packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : MySQL vulnerabilities (USN-7245-1) (214820)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 31 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenSSH vulnerabilities (USN-7270-1) (216422)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Python vulnerability (USN-7280-1) (216590)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Raptor vulnerabilities (USN-7316-1) (217185)]

+ Action to take : Update the affected libraptor2-0, libraptor2-dev and / or raptor2-utils packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerability (USN-7220-1) (232304)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : X.Org X Server vulnerabilities (USN-7299-1) (216771)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : curl vulnerability (USN-7162-1) (213082)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libarchive vulnerability (USN-7087-1) (209984)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libcap2 vulnerability (USN-7287-1) (216701)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7432-1) (234139)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : mpg123 vulnerability (USN-7092-1) (210368)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerabilities (USN-7426-1) (234054)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : wpa_supplicant and hostapd vulnerabilities (USN-7317-1) (218383)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Apache HTTP Server vulnerability (USN-6902-1) (202614)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Bind vulnerabilities (USN-6909-1) (203144)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : BusyBox vulnerabilities (USN-6961-1) (205548)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : CUPS vulnerability (USN-7041-1) (207842)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Flatpak and Bubblewrap vulnerability (USN-7046-1) (207953)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : GNOME Shell vulnerability (USN-6963-1) (205629)]

+ Action to take : Update the affected gnome-shell, gnome-shell-common and / or gnome-shell-extension-prefs packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : GTK vulnerability (USN-6899-1) (202475)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Ghostscript vulnerabilities (USN-6897-1) (202378)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : LibreOffice vulnerability (USN-6962-1) (205630)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : MySQL vulnerabilities (USN-6934-1) (204922)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : ORC vulnerability (USN-6964-1) (205640)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Python vulnerabilities (USN-7015-1) (207282)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-7012-1) (207281)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : libgsf vulnerabilities (USN-7062-1) (208701)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : snapd vulnerabilities (USN-6940-1) (204952)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS / 24.10 : libtasn1 vulnerability (USN-7275-1) (216431)]

+ Action to take : Update the affected libtasn1-6, libtasn1-6-dev and / or libtasn1-bin packages.

[Ubuntu 20.04 LTS / 22.04 LTS / 24.10 : Vim vulnerability (USN-7261-1) (215238)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : AccountsService vulnerability (USN-6687-1) (191789)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : AppArmor vulnerability (USN-7035-1) (207768)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : Bind vulnerabilities (USN-5827-1) (170632)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-7222-1) (214506)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : FLAC vulnerability (USN-6360-1) (181316)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : FreeType vulnerability (USN-7352-1) (232846)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : GDK-PixBuf vulnerability (USN-5607-1) (165011)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : GLib vulnerabilities (USN-6165-1) (177323)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6655-1) (191003)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : GnuTLS vulnerability (USN-5901-1) (171967)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : HarfBuzz vulnerability (USN-7251-1) (214894)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerability (USN-7025-1) (207457)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6172-1) (183722)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : MariaDB vulnerabilities (USN-5739-1) (168154)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 36 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1) (189773)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : Pillow vulnerabilities (USN-5777-1) (168673)]

+ Action to take : Update the affected python3-pil and / or python3-pil.imagetk packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerability (USN-7218-1) (214444)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : Samba vulnerabilities (USN-5993-1) (173794)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerability (USN-7193-1) (213601)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5893-1) (171943)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 28 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : cups-filters vulnerabilities (USN-7043-4) (208473)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS / 22.04 LTS : ldb vulnerability (USN-5992-1) (173795)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS / 22.04 LTS : zlib vulnerability (USN-5570-2) (166179)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS : AccountsService vulnerability (USN-5149-1) (155374)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS : Bind vulnerabilities (USN-6642-1) (190715)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS : Ceph vulnerabilities (USN-4998-1) (151000)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

```
[ Ubuntu 20.04 LTS : Exiv2 regression (USN-5043-2) (156633) ]
+ Action to take : Update the affected exiv2, libexiv2-27 and / or libexiv2-dev packages.

[ Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7334-1) (232218) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 262 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : GDK-PixBuf vulnerability (USN-5554-1) (163921) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : GNOME Shell vulnerability (USN-4464-1) (139692) ]
+ Action to take : Update the affected gnome-shell, gnome-shell-common and / or gnome-shell-extension-prefs packages.

[ Ubuntu 20.04 LTS : GNU binutils vulnerability (USN-6160-1) (177263) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS : GUPnP vulnerability (USN-4970-1) (150130) ]
+ Action to take : Update the affected gir1.2-gupnp-1.2, libgupnp-1.2-0 and / or libgupnp-1.2-dev packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : Ghostscript vulnerability (USN-5075-1) (153211) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS : GnuTLS vulnerabilities (USN-5029-1) (152181) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : HPLIP vulnerability (USN-7202-1) (214007) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS : ICU vulnerability (USN-5156-1) (155722) ]
+ Action to take : Update the affected icu-devtools, libicu-dev and / or libicu66 packages.

[ Ubuntu 20.04 LTS : LibRaw vulnerability (USN-6377-1) (181541) ]
+ Action to take : Update the affected libraw-bin, libraw-dev and / or libraw19 packages.

[ Ubuntu 20.04 LTS : LibTIFF vulnerability (USN-5084-1) (153508) ]
+ Action to take : Update the affected packages.

[ Ubuntu 20.04 LTS : LibreOffice vulnerabilities (USN-5661-1) (165731) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5294-1) (158159) ]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[ Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5589-1) (164529) ]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1) (173619) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-7003-1) (207055) ]  
+ Action to take : Update the affected kernel package.  
+Impact : Taking this action will resolve 85 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : MariaDB vulnerabilities (USN-5305-1) (158456) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : OpenJPEG vulnerabilities (USN-4685-1) (144788) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : OpenSSH vulnerability (USN-4762-1) (147985) ]  
+ Action to take : Update the affected packages.
```

```
[ Ubuntu 20.04 LTS : PolicyKit vulnerability (USN-5304-1) (158455) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : PyYAML vulnerability (USN-4940-1) (149417) ]  
+ Action to take : Update the affected python-yaml and / or python3-yaml packages.
```

```
[ Ubuntu 20.04 LTS : Python vulnerabilities (USN-5201-1) (183724) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : Samba vulnerabilities (USN-5936-1) (172367) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : Squashfs-Tools vulnerability (USN-5078-3) (154053) ]  
+ Action to take : Update the affected squashfs-tools package.
```

```
[ Ubuntu 20.04 LTS : Thunderbird vulnerabilities (USN-4995-1) (150949) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 25 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : Vim regression (USN-5613-2) (165247) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5394-1) (160307) ]  
+ Action to take : Update the affected packages.  
+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).
```

```
[ Ubuntu 20.04 LTS : cryptsetup vulnerability (USN-5286-1) (158072) ]  
+ Action to take : Update the affected packages.
```

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS : libarchive vulnerability (USN-5374-1) (159645)]

+ Action to take : Update the affected libarchive-dev, libarchive-tools and / or libarchive13 packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS : libmaxminddb vulnerability (USN-4631-1) (142866)]

+ Action to take : Update the affected libmaxminddb-dev, libmaxminddb0 and / or mddb-bin packages.

[Ubuntu 20.04 LTS : libssh vulnerability (USN-5053-1) (152869)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS : libuv vulnerability (USN-5007-1) (151443)]

+ Action to take : Update the affected libuv1 and / or libuv1-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS : mpg123 vulnerability (USN-7092-2) (211912)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS : snapd vulnerabilities (USN-5292-2) (158160)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 20.04 LTS : systemd vulnerability (USN-5226-1) (156711)]

+ Action to take : Update the affected packages.

[Ubuntu 20.04 LTS : urllib3 vulnerability (USN-5812-1) (170179)]

+ Action to take : Update the affected python3-urllib3 package.

[Ubuntu 20.04 LTS : util-linux vulnerabilities (USN-5279-1) (157843)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2024/07/24

Plugin Output

tcp/0

The following global addresss were gathered :

- 2409:40c0:106b:64d2:e68a:b2fc:9941:9ce2
- 2409:40c0:106b:64d2:1bf:5adb:5e83:320

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

Nessus negotiated the following encryption algorithm(s) with the server :

Client to Server: aes256-ctr
Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for kex_algorithms :

curve25519-sha256

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

The server supports the following options for compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for encryption_algorithms_server_to_client :

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

| | |
|------|------------------|
| XREF | IAVB:0001-B-0507 |
|------|------------------|

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : silky
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C dmidecode"
Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
- Command : "LC_ALL=C /sbin/dmidecode"
Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
- Plugin Filename : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
- Command : "/usr/sbin/dmidecode -s system-version 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : enumerate_oci_nix.nasl
Plugin ID : 154138
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
```

```
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Command : "LC_ALL=C /sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : host_tag_nix.nbin
Plugin ID : 87414
Plugin Name : Host Tagging (Linux)
- Command : "sh -c \"echo d659ce491658490b8243879f93b606a1 > /etc/enable_tag && echo OK\""
Response : null
Error : "\nsh: 1: cannot create /etc/enable_tag: Permission denied"
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled**Synopsis**

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etc@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etc@openssh.com

10267 - SSH Server Type and Version Information**Synopsis**

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
SSH supported authentication : publickey,password
```

25240 - Samba Server Detection**Synopsis**

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

<https://www.samba.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

tcp/445/cifs

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

An SSH server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

A web server is running on this port.

22869 - Software Enumeration (SSH)**Synopsis**

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

Here is the list of packages installed on the remote Debian Linux system :

```
ii accountsservice 0.6.55-0ubuntu12~20.04.1 amd64 query and manipulate user account information
ii acl 2.2.53-6 amd64 access control list - utilities
ii acpi-support 0.143 amd64 scripts for handling many ACPI events
ii acpid 1:2.0.32-1ubuntu1 amd64 Advanced Configuration and Power Interface event daemon
ii adduser 3.118ubuntu2 all add and remove users and groups
ii adwaita-icon-theme 3.36.1-2ubuntu0.20.04.2 all default icon theme of GNOME (small subset)
ii aisleriot 1:3.22.9-1 amd64 GNOME solitaire card game collection
ii alsa-base 1.0.25+dfsg-0ubuntu5 all ALSA driver configuration files
ii alsa-topology-conf 1.2.2-1 all ALSA topology configuration files
ii alsa-ucm-conf 1.2.2-1ubuntu0.1 all ALSA Use Case Manager configuration files
ii alsa-utils 1.2.2-1ubuntu1 amd64 Utilities for configuring and using ALSA
ii amd64-microcode 3.20191218.1ubuntu1 amd64 Processor microcode firmware for AMD CPUs
ii anacron 2.3-29 amd64 cron-like program that doesn't go by time
ii apache2 2.4.41-4ubuntu3 amd64 Apache HTTP Server
ii apache2-bin 2.4.41-4ubuntu3 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.41-4ubuntu3 all Apache HTTP Server (common files)
ii apache2-utils 2.4.41-4ubuntu3 amd64 Apache HTTP Server (utility programs for web servers)
ii app 2.2.3.dfsg.1-5 amd64 Automated Password Generator - Standalone version
ii app-install-data-partner 19.04 all Application Installer (data files for partner applications/repositories)
```

```

ii apparmor 2.13.3-7ubuntu5.1 amd64 user-space parser utility for AppArmor
ii apport 2.20.11-0ubuntu27.4 all automatically generate crash reports for debugging
ii apport-gtk 2.20.11-0ubuntu27.4 all GTK+ frontend for the apport crash report system
ii apport-symptoms 0.23 all symptom scripts for apport
ii appstream 0.12.10-2 amd64 Software component metadata management
ii apt 2.0.2ubuntu0.1 amd64 commandline package manager
ii apt-config-icons 0.12.10-2 all APT configuration snippet to enable icon downloads
ii apt-config-icons-hidpi 0.12.10-2 all APT configuration snippet to enable HiDPI icon downloads
ii apt-utils 2.0.2ubuntu0.1 amd64 package management related utility programs
ii aptdaemon 1.1.1+bzr982-0ubuntu32.1 all transaction based package management service
ii aptdaemon-data 1.1.1+bzr982-0ubuntu32.1 all data files for clients
ii apturl 0.5.2ubuntu19 amd64 install packages using the apt protocol - GTK+ frontend
ii apturl-common 0.5.2ubuntu19 amd64 install packages using the apt protocol - common data
ii aspell 0.60.8-1build1 amd64 GNU Aspell spell-checker
ii aspell-en 2018.04.16-0-1 all English dictionary for GNU Aspell
ii at-sp2-core 2.36.0-2 amd64 Assistive Technology Service Provider Interface (dbus core)
ii attr 1:2.4.48-5 amd64 utilities for manipulating filesystem extended attributes
ii autoconf 2.69-11.1 all automatic configure script builder
ii automake 1:1.16.1-4ubuntu6 all Tool for generating GNU Standards-compliant Makefiles
ii autopoint 0.19.8.1-10build1 all autopoint program from GNU gettext
ii autotools-dev 20180224.1 all Update infrastructure for config.{guess,sub} files
ii avahi-autoipd 0.7-4ubuntu7 amd64 Avahi IPv4LL network address configuration daemon
ii avahi-daemon 0.7-4ubuntu7 amd64 Avahi mDNS/DNS-SD daemon
ii avahi-utils 0.7-4ubuntu7 amd64 Avahi browsing, publishing and discovery utilities
ii baobab 3.34.0-1 amd64 GNOME disk usage analyzer
ii base-files 11ubuntu5.1 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.47 amd64 Debian base system master password and group files
ii bash 5.0-6ubuntu1.1 amd64 GNU Bourne Again SHell
ii bash-completion 1:2.10-1ubuntu1 all programmable completion for the bash shell
ii bc 1.07.1-2build1 amd64 GNU bc arbitrary precision calculator language
ii bind9-dnsutils 1:9.16.1-0ubuntu2.2 amd64 Clients provided with BIND 9
ii bind9-host 1:9.16.1-0ubuntu2.2 amd64 DNS Lookup Utility
ii bind9-libs 1:9.16.1-0ubuntu2.2 amd64 Shared Libraries used by BIND 9
ii binutils 2.34-6ubuntu1 amd64 GNU assembler, linker and binary utilities
ii binutils-common 2.34-6ubuntu1 amd64 Common files for the GNU assembler, linker and binary utilities
ii binutils-x86-64-linux-gnu 2.34-6ubuntu1 amd64 GNU binary utilities, for x86-64-linux-gnu target
ii bluez 5.53-0ubuntu3 amd64 Bluetooth tools and daemons
ii bluez-cups 5.53-0ubuntu3 amd64 Bluetooth printer driver for CUPS
ii bluez-obexd 5.53-0ubuntu3 amd64 bluez obex daemon
ii bolt 0.8-4 amd64 system daemon to manage thunderbolt 3 devices
ii branding-ubuntu 0.10 all Replacement artwork with Ubuntu branding
ii brltty 6.0+dfsg-4ubuntu6 amd64 Access software for a blind person using a braille display
ii bsdmainutils 11.1.2ubuntu3 amd64 collection of more utilities from FreeBSD
ii bsdtar 1:2.34-0.1ubuntu9 amd64 basic utilities from 4.4BSD-Lite
ii bubblewrap 0.4.0-1ubuntu4 amd64 setuid wrapper for unprivileged chroot and namespace manipulation
ii build-essential 12.8ubuntu1 amd64 Informational list of build-essential packages
ii busybox-initramfs 1:1.30.1-4ubuntu6.1 amd64 Standalone shell setup for initramfs
ii busybox-static 1:1.30.1-4ubuntu6.1 amd64 Standalone rescue shell with tons of builtin utilities
ii bzip2 1.0.8-2 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20190110ubuntu1.1 all Common CA certificates
ii cheese 3.34.0-1build1 amd64 tool to take pictures and videos from your webcam
ii cheese-common 3.34.0-1build1 all Common files for the Cheese tool to take pictures and videos
ii colord 1.4.4-2 amd64 system service to manage device colour profiles -- system daemon
ii colord-data 1.4.4-2 all system service to manage device colour profiles -- data files
ii command-not-found 20.04.2 all Suggest installation of packages in interactive bash sessions
ii console-setup 1.194ubuntu3 all console font and keymap setup program
ii console-setup-linux 1.194ubuntu3 all Linux specific part of console-setup
ii coreutils 8.30-3ubuntu2 amd64 GNU core utilities
ii cpio 2.13+dfsg-2 amd64 GNU cpio -- a program to manage archives of files
ii cpp 4.9.3.0-1ubuntu2 amd64 GNU C preprocessor (cpp)
ii cpp-9 9.3.0-10ubuntu2 amd64 GNU C preprocessor
ii cracklib-runtime 2.9.6-3.2 amd64 runtime support for password checker library cracklib2
ii crda 3.18-1build1 amd64 wireless Central Regulatory Domain Agent
ii cron 3.0pl1-136ubuntu1 amd64 process scheduling daemon
ii cups 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - PPD/driver support, web interface
ii cups-browsed 1.27.4-1 amd64 OpenPrinting CUPS Filters - cups-browsed
ii cups-bsd 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - BSD commands
ii cups-client 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - client programs (SysV)
ii cups-common 2.3.1-9ubuntu1.1 all Common UNIX Printing System(tm) - common files
ii cups-core-drivers 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - driverless printing
ii cups-daemon 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - daemon
ii cups-filters 1.27.4-1 amd64 OpenPrinting CUPS Filters - Main Package
ii cups-filters-core-drivers 1.27.4-1 amd64 OpenPrinting CUPS Filters - Driverless printing
ii cups-ipp-utils 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - IPP developer/admin utilities
ii cups-pk-helper 0.2.6-1ubuntu3 amd64 PolicyKit helper to configure cups with fine-grained privileges
ii cups-pdcd 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - PPD manipulation utilities
ii cups-server-common 2.3.1-9ubuntu1.1 all Common UNIX Printing System(tm) - server common files
ii dash 0.5.10-2-6 amd64 POSIX-compliant shell
ii dbus 1.12.16-2ubuntu2.1 amd64 simple interprocess messaging system (daemon and utilities)
ii dbus-user-session 1.12.16-2ubuntu2.1 amd64 simple interprocess messaging system (systemd --user integration)
ii dbus-x11 1.12.16-2ubuntu2.1 amd64 simple interprocess messaging system (X11 deps)
ii dc 1.07.1-2build1 amd64 dc arbitrary precision reverse-polish calculator
ii dconf-cli 0.36.0-1 amd64 simple configuration storage system - utilities
ii dconf-gsettings-backend 0.36.0-1 amd64 simple configuration storage system - GSettings back-end
ii dconf-service 0.36.0-1 amd64 simple configuration storage system - D-Bus service
ii debconf 1.5.73 all Debian configuration management system
ii debconf-i18n 1.5.73 all full internationalization support for debconf
ii debhelper 12.10ubuntu1 all helper programs for debian/rules
ii debianutils 4.0.1 amd64 Miscellaneous utilities specific to Debian
ii dejá-dup 40.7-0ubuntu1 amd64 Backup utility
ii desktop-file-utils 0.24-1ubuntu3 amd64 Utilities for .desktop files
ii dh-autoreconf 19 all debhelper add-on to call autoreconf and clean up after the build
ii dh-strip-nondeterminism 1.7.0-1 all file non-deterministic information stripper - Debhelper add-on
ii dictionaries-common 1.28.1 all spelling dictionaries - common utilities
ii diffutils 1:3.7-3 amd64 File comparison utilities
ii dirmngr 2.2.19-3ubuntu2 amd64 GNU privacy guard - network certificate management service
ii distro-info-data 0.43ubuntu1.1 all information about the distributions' releases (data files)
ii dmidecode 3.2-3 amd64 SMBIOS/DMI table decoder
ii dmsetup 2:1.02.167-1ubuntu1 amd64 Linux Kernel Device Mapper userspace library

```

```

ii dmz-cursor-theme 0.4.5ubuntu1 all Style neutral, scalable cursor theme
ii dns-root-data 2019052802 all DNS root data including root zone and DNSSEC key
ii dnsmasq-base 2.80-1.1ubuntu1 amd64 Small caching DNS proxy and DHCP/TFTP server
ii docbook-xml 4.5-9 all standard XML documentation system for software and systems
ii dosfstools 4.1-2 amd64 utilities for making and checking MS-DOS FAT filesystems
ii dpkg 1.19.7ubuntu3 amd64 Debian package management system
ii dpkg-dev 1.19.7ubuntu3 all Debian package development tools
ii duplicity 0.8.11.1612-1 amd64 encrypted bandwidth-efficient backup
ii dwz 0.13-5 amd64 DWARF compression tool
ii e2fsprogs 1.45.5-2ubuntu1 amd64 ext2/ext3/ext4 file system utilities
ii ed 1.16-1 amd64 classic UNIX line editor
ii eject 2.1.5+deb1+cvs20081104-14 amd64 ejects CDs and operates CD-Changers under Linux
ii emacsclient 3.0.4 all Common facilities for all emacsen
ii enchant-2 2.2.8-1 amd64 Wrapper for various spell checker engines (binary programs)
ii eog 3.36.3-0ubuntu1 amd64 Eye of GNOME graphics viewer program
ii espeak-ng-data 1.50+dfsg-6 amd64 Multi-lingual software speech synthesizer: speech data files
ii evince 3.36.7-0ubuntu1 amd64 Document (PostScript, PDF) viewer
ii evince-common 3.36.7-0ubuntu1 all Document (PostScript, PDF) viewer - common files
ii evolution-data-server 3.36.3-0ubuntu1.1 amd64 evolution database backend server
ii evolution-data-server-common 3.36.3-0ubuntu1.1 all architecture independent files for Evolution Data Server
ii fakeroot 1.24-1 amd64 tool for simulating superuser privileges
ii fdisk 2.34-0.1ubuntu9 amd64 collection of partitioning utilities
ii file 1:5.38-4 amd64 Recognize the type of data in a file using "magic" numbers
ii file-roller 3.36.2-0ubuntu1 amd64 archive manager for GNOME
ii findutils 4.7.0-1ubuntu1 amd64 utilities for finding files--find, xargs
ii firefox 78.0.2+build2-0ubuntu0.20.04.1 amd64 Safe and easy web browser from Mozilla
ii firefox-locale-de 78.0.2+build2-0ubuntu0.20.04.1 amd64 German language pack for Firefox
ii firefox-locale-en 78.0.2+build2-0ubuntu0.20.04.1 amd64 English language pack for Firefox
ii fontconfig 2.13.1-2ubuntu3 amd64 generic font configuration library - support binaries
ii fontconfig-config 2.13.1-2ubuntu3 all generic font configuration library - configuration
ii fonts-beng 2:1.2 all Metapackage to install Bengali and Assamese fonts
ii fonts-beng-extra 1.0-7 all TrueType fonts for Bengali language
ii fonts-dejavu-core 2.37-1 all Vera font family derivates with additional characters
ii fonts-deva 2:1.2 all Meta package to install all Devanagari fonts
ii fonts-deva-extra 3.0-5 all Free fonts for Devanagari script
ii fonts-droid-fallback 1:6.0.1r16-1.1 all handheld device font with extensive style and language support (fallback)
ii fonts-freefont-ttf 20120503-10 all Freefont Serif, Sans and Mono Truetype fonts
ii fonts-gargi 2.0-4 all OpenType Devanagari font
ii fonts-gubbi 1.3-3 all Gubbi free font for Kannada script
ii fonts-gujr 2:1.3 all Meta package to install all Gujarati fonts
ii fonts-gujr-extra 1.0.1-1 all Free fonts for Gujarati script
ii fonts-guru 2:1.2 all Meta package to install all Punjabi fonts
ii fonts-guru-extra 2.0-5 all Free fonts for Punjabi language
ii fonts-indic 2:1.3 all Meta package to install all Indian language fonts
ii fonts-kacst 2.01+mry-14 all KACST free TrueType Arabic fonts
ii fonts-kacst-one 5.0+svn11846-10 all TrueType font designed for Arabic language
ii fonts-kalapi 1.0-3 all Kalapi Gujarati Unicode font
ii fonts-khmeros-core 5.0-7ubuntu1 all KhmerOS Unicode fonts for the Khmer language of Cambodia
ii fonts-knda 2:1.2 all Meta package for Kannada fonts
ii fonts-lao 0.0.20060226-9ubuntu1 all TrueType font for Lao language
ii fonts-liberation 1:1.07.4-11 all Fonts with the same metrics as Times, Arial and Courier
ii fonts-liberation2 2.1.0-1 all Fonts with the same metrics as Times, Arial and Courier (v2)
ii fonts-lklug-sinhala 0.6-3 all Unicode Sinhala font by Lanka Linux User Group
ii fonts-lohit-beng-assamese 2.91.5-1 all Lohit TrueType font for Assamese Language
ii fonts-lohit-beng-bengali 2.91.5-1 all Lohit TrueType font for Bengali Language
ii fonts-lohit-deva 2.95.4-4 all Lohit TrueType font for Devanagari script
ii fonts-lohit-gujr 2.92.4-4 all Lohit TrueType font for Gujarati Language
ii fonts-lohit-guru 2.91.2-1 all Lohit TrueType font for Punjabi Language
ii fonts-lohit-knda 2.5.4-2 all Lohit TrueType font for Kannada Language
ii fonts-lohit-mlym 2.92.2-1 all Lohit TrueType font for Malayalam Language
ii fonts-lohit-orya 2.91.2-1 all Lohit TrueType font for Oriya Language
ii fonts-lohit-taml 2.91.3-1 all Lohit TrueType font for Tamil Language
ii fonts-lohit-taml-classical 2.5.4-1 all Lohit Tamil TrueType fonts for Tamil script
ii fonts-lohit-telu 2.5.5-1 all Lohit TrueType font for Telugu Language
ii fonts-mlym 2:1.2 all Meta package to install all Malayalam fonts
ii fonts-nakula 1.0-3 all Free Unicode compliant Devanagari font
ii fonts-navili 1.2-2 all Handwriting font for Kannada
ii fonts-noto-cjk 1:20190410+repack1-2 all "No Tofu" font families with large Unicode coverage (CJK regular and bold)
ii fonts-noto-color-emoji 0~20200408-1 all color emoji font from Google
ii fonts-noto-mono 20200323-1 all "No Tofu" monospaced font family with large Unicode coverage
ii fonts-opensymbol 2:102.11+Lib06.4.4-0ubuntu0.20.04.1 all OpenSymbol TrueType font
ii fonts-orya 2:1.2 all Meta package to install all Oriya fonts
ii fonts-orya-extra 2.0-6 all Free fonts for Odia script
ii fonts-pagul 1.0-7 all Free TrueType font for the Sourashtra language
ii fonts-sahadeva 1.0-4 all Free Unicode compliant Devanagari font
ii fonts-samyak-deva 1.2.2-4 all Samyak TrueType font for Devanagari script
ii fonts-samyak-gujr 1.2.2-4 all Samyak TrueType font for Gujarati language
ii fonts-samyak-mlym 1.2.2-4 all Samyak TrueType font for Malayalam language
ii fonts-samyak-taml 1.2.2-4 all Samyak TrueType font for Tamil language
ii fonts-sarai 1.0-2 all truetype font for devanagari script
ii fonts-sil-abyssinica 2.000-1 all Unicode font for the Ethiopic script
ii fonts-sil-padauk 4.000-1 all Burmese Unicode TrueType font with OpenType and Graphite support
ii fonts-smc 1:7.1 all Metapackage for various TrueType fonts for Malayalam Language
ii fonts-smc-anjalioldlipi 7.1.2-1 all AnjaliOldLipi malayalam font
ii fonts-smc-chilanka 1.400-1 all Chilanka malayalam font
ii fonts-smc-dyuthi 3.0.2-1 all Dyuthi malayalam font
ii fonts-smc-gayathri 1.100-1 all Gayathri Malayalam font
ii fonts-smc-karumbi 1.1.2-1 all Karumbi malayalam font
ii fonts-smc-keraleeyam 3.0.2-1 all Keraleeyam malayalam font
ii fonts-smc-manjari 1.710-1 all Manjari malayalam font
ii fonts-smc-meera 7.0.3-1 all Meera malayalam font
ii fonts-smc-rachana 7.0.2-1 all Rachana malayalam font
ii fonts-smc-raghumaMalayalamSans 2.2.1-1 all RaghumaMalayalamSans malayalam font
ii fonts-smc-suruma 3.2.3-1 all Suruma malayalam font
ii fonts-smc-uuroob 2.0.2-1 all Uuroob malayalam font
ii fonts-taml 2:1.3 all Meta package to install all Tamil fonts
ii fonts-telu 2:1.2 all Meta package to install all Telugu fonts
ii fonts-telu-extra 2.0-4 all Free fonts for Telugu script
ii fonts-thai-tlwg 1:0.7.1-3 all Thai fonts maintained by TLWG (metapackage)

```

```

ii fonts-tibetan-machine 1.901b-5 all font for Tibetan, Dzongka and Ladakhi (OpenType Unicode)
ii fonts-tlwg-garuda 1:0.7.1-3 all Thai Garuda font (dependency package)
ii fonts-tlwg-garuda-ttf 1:0.7.1-3 all Thai Garuda TrueType font
ii fonts-tlwg-kinnari 1:0.7.1-3 all Thai Kinnari font (dependency package)
ii fonts-tlwg-kinnari-ttf 1:0.7.1-3 all Thai Kinnari TrueType font
ii fonts-tlwg-laksaman 1:0.7.1-3 all Thai Laksaman font (dependency package)
ii fonts-tlwg-laksaman-ttf 1:0.7.1-3 all Thai Laksaman TrueType font
ii fonts-tlwg-loma 1:0.7.1-3 all Thai Loma font (dependency package)
ii fonts-tlwg-loma-ttf 1:0.7.1-3 all Thai Loma TrueType font
ii fonts-tlwg-mono 1:0.7.1-3 all Thai TlwgMono font (dependency package)
ii fonts-tlwg-mono-ttf 1:0.7.1-3 all Thai TlwgMono TrueType font
ii fonts-tlwg-norasi 1:0.7.1-3 all Thai Norasi font (dependency package)
ii fonts-tlwg-norasi-ttf 1:0.7.1-3 all Thai Norasi TrueType font
ii fonts-tlwg-purisa 1:0.7.1-3 all Thai Purisa font (dependency package)
ii fonts-tlwg-purisa-ttf 1:0.7.1-3 all Thai Purisa TrueType font
ii fonts-tlwg-sawasdee 1:0.7.1-3 all Thai Sawasdee font (dependency package)
ii fonts-tlwg-sawasdee-ttf 1:0.7.1-3 all Thai Sawasdee TrueType font
ii fonts-tlwg-typewriter 1:0.7.1-3 all Thai TlwgTypewriter font (dependency package)
ii fonts-tlwg-typewriter-ttf 1:0.7.1-3 all Thai TlwgTypewriter TrueType font
ii fonts-tlwg-typist 1:0.7.1-3 all Thai TlwgTypist font (dependency package)
ii fonts-tlwg-typist-ttf 1:0.7.1-3 all Thai TlwgTypist TrueType font
ii fonts-tlwg-typo 1:0.7.1-3 all Thai TlwgTypo font (dependency package)
ii fonts-tlwg-typo-ttf 1:0.7.1-3 all Thai TlwgTypo TrueType font
ii fonts-tlwg-umpush 1:0.7.1-3 all Thai Umpush font (dependency package)
ii fonts-tlwg-umpush-ttf 1:0.7.1-3 all Thai Umpush TrueType font
ii fonts-tlwg-waree 1:0.7.1-3 all Thai Waree font (dependency package)
ii fonts-tlwg-waree-ttf 1:0.7.1-3 all Thai Waree TrueType font
ii fonts-ubuntu 0.83-4ubuntu1 all sans-serif font set from Ubuntu
ii fonts-urw-base35 20170801.1-3 all font set metric-compatible with the 35 PostScript Level 2 Base Fonts
ii fonts-yrsa-rasa 1.002-2 all Open-source, libre fonts for Latin + Gujarati
ii foomatic-db-compressed-ppds 20200401-1 all OpenPrinting printer support - Compressed PPDs derived from the database
ii fprintd 1.90.1-1ubuntu1 amd64 D-Bus daemon for fingerprint reader access
ii friendly-recovery 0.2.41 all Make recovery boot mode more user-friendly
ii ftp 0.17-34.1 amd64 classical file transfer client
ii fuse 2.9.9-3 amd64 Filesystem in Userspace
ii fwupd 1.3.11-1-focal1 amd64 Firmware update daemon
ii fwupd-signed 1.27.1ubuntu2+1.3.11-1-focal1 amd64 Linux Firmware Updater EFI signed binary
ii g++ 4.9.3.0-1ubuntu2 amd64 GNU C++ compiler
ii g++-9 9.3.0-10ubuntu2 amd64 GNU C++ compiler
ii galera-3 25.3.29-1 amd64 Replication framework for transactional applications
ii gamemode 1.5.1-0ubuntu3.1 amd64 Optimise Linux system performance on demand
ii gawk 1:5.0.1+dfsg-1 amd64 GNU awk, a pattern scanning and processing language
ii gcc 4:9.3.0-1ubuntu2 amd64 GNU C compiler
ii gcc-10-base 10-20200411-0ubuntu1 amd64 GCC, the GNU Compiler Collection (base package)
ii gcc-9 9.3.0-10ubuntu2 amd64 GNU C compiler
ii gcc-9-base 9.3.0-10ubuntu2 amd64 GCC, the GNU Compiler Collection (base package)
ii gcr 3.36.0-2build1 amd64 GNOME crypto services (daemon and tools)
ii gdb 9.1-0ubuntu1 amd64 GNU Debugger
ii gdbserver 9.1-0ubuntu1 amd64 GNU Debugger (remote server)
ii gdisk 1.0.5-1 amd64 GPT fdisk text-mode partitioning tool
ii gdm3 3.34.1-1ubuntu1 amd64 GNOME Display Manager
ii gedit 3.36.2-0ubuntu1 amd64 official text editor of the GNOME desktop environment
ii gedit-common 3.36.2-0ubuntu1 all official text editor of the GNOME desktop environment (support files)
ii genisoimage 9:1.1.11-3.1ubuntu1 amd64 Creates ISO-9660 CD-ROM filesystem images
ii geoclue-2.0 2.5.6-0ubuntu1 amd64 geoinformation service
ii gettext 0.19.8.1-10build1 amd64 GNU Internationalization utilities
ii gettext-base 0.19.8.1-10build1 amd64 GNU Internationalization utilities for the base system
ii ghostscript 9.50+dfsg-5ubuntu4 amd64 interpreter for the PostScript language and for PDF
ii ghostscript-x 9.50+dfsg-5ubuntu4 amd64 interpreter for the PostScript language and for PDF - X11 support
ii gir1.2-accountsservice-1.0 0.6.55-0ubuntu12~20.04.1 amd64 GObject introspection data for AccountService
ii gir1.2-atk-1.0 2.35.1-1ubuntu2 amd64 ATK accessibility toolkit (GObject introspection)
ii gir1.2-atspi2-2.0 2.36.0-2 amd64 Assistive Technology Service Provider (GObject introspection)
ii gir1.2-dbusmenu-glib-0.4 16.04.1+18.10.20180917-0ubuntu6 amd64 typelib file for libdbusmenu-glib4
ii gir1.2-dee-1.0 1.2.7+17.10.20170616-4ubuntu6 amd64 GObject introspection data for the Dee library
ii gir1.2-freeesktop 1.64.1-1~ubuntu20.04.1 amd64 Introspection data for some FreeDesktop components
ii gir1.2-gck-1 3.36.0-2build1 amd64 GObject introspection data for the GCK library
ii gir1.2-gcr-3 3.36.0-2build1 amd64 GObject introspection data for the GCR library
ii gir1.2-gdesktoptenums-3.0 3.36.0-1ubuntu1 amd64 GObject introspection for GSettings desktop-wide schemas
ii gir1.2-gdkpixbuf-2.0 2.40.0+dfsg-3 amd64 GDK Pixbuf library - GObject-Introspection
ii gir1.2-gdm-1.0 3.34.1-1ubuntu1 amd64 GObject introspection data for the GNOME Display Manager
ii gir1.2-geoclue-2.0 2.5.6-0ubuntu1 amd64 convenience library to interact with geoinformation service (introspection)
ii gir1.2-glib-2.0 1.64.1-1~ubuntu20.04.1 amd64 Introspection data for GLib, GObject, Gio and GModule
ii gir1.2-gmenu-3.0 3.36.0-1ubuntu1 amd64 GObject introspection data for the GNOME menu library
ii gir1.2-gnombuetooth-1.0 3.34.1-1 amd64 Introspection data for GnomeBluetooth
ii gir1.2-gnomedesktop-3.0 3.36.3.1-0ubuntu1 amd64 Introspection data for GnomeDesktop
ii gir1.2-goa-1.0 3.36.0-1ubuntu1 amd64 Introspection data for GNOME Online Accounts
ii gir1.2-graphene-1.0 1.10.0-1build2 amd64 library of graphic data types (introspection files)
ii gir1.2-gst-plugins-base-1.0 1.16.2-4 amd64 GObject introspection data for the GStreamer Plugins Base library
ii gir1.2-gstreamer-1.0 1.16.2-2 amd64 GObject introspection data for the GStreamer library
ii gir1.2-gtk-3.0 3.24.20-0ubuntu1 amd64 GTK graphical user interface library -- gir bindings
ii gir1.2-gtksource-4 4.6.0-1 amd64 gir files for the GTK+ syntax highlighting widget
ii gir1.2-gudev-1.0 1:233-1 amd64 libgudev-1.0 introspection data
ii gir1.2-gweather-3.0 3.36.0-1 amd64 GObject introspection data for the GWeather library
ii gir1.2-ibus-1.0 1.5.22-2ubuntu2.1 amd64 Intelligent Input Bus - introspection data
ii gir1.2-javascriptcoregtk-4.0 2.28.3-0ubuntu0.20.04.1 amd64 JavaScript engine library from WebKitGTK - GObject introspection data
ii gir1.2-json-1.0 1.4.4-2ubuntu2 amd64 GLib JSON manipulation library (introspection data)
ii gir1.2-mutter-6 3.36.3-0ubuntu0.20.04.1 amd64 GObject introspection data for Mutter
ii gir1.2-nm-1.0 1.22.10-1ubuntu2.1 amd64 GObject introspection data for the libnm library
ii gir1.2-nma-1.0 1.8.24-1ubuntu2 amd64 GObject introspection data for libnma
ii gir1.2-notify-0.7 0.7.9-1ubuntu2 amd64 sends desktop notifications to a notification daemon (Introspection files)
ii gir1.2-packagekitglib-1.0 1.1.13-2ubuntu1 amd64 GObject introspection data for the PackageKit GLib library
ii gir1.2-pango-1.0 1.44.7-2ubuntu4 amd64 Layout and rendering of internationalized text - gir bindings
ii gir1.2-peas-1.0 1.26.0-2 amd64 Application plugin library (introspection files)
ii gir1.2-polkit-1.0 0.105-26ubuntu1 amd64 GObject introspection data for PolicyKit
ii gir1.2-rb-3.0 3.4.4-1ubuntu2 amd64 GObject introspection data for the rhythmbox music player
ii gir1.2-rsvg-2.0 2.48.7-1ubuntu0.20.04.1 amd64 gir files for renderer library for SVG files
ii gir1.2-secret-1 0.20.3-0ubuntu1 amd64 Secret store (GObject-Introspection)
ii gir1.2-snapd-1 1.57-0ubuntu3 amd64 TypeLib file for libsnappy-glib
ii gir1.2-soup-2.4 2.70.0-1 amd64 GObject introspection data for the libsoup HTTP library

```

```

ii gir1.2-totem-1.0 3.34.1-2ubuntu2 amd64 GObject introspection data for Totem media player
ii gir1.2-totemparser-1.0 3.26.5-1ubuntu1 amd64 GObject introspection data for the Totem Playlist Parser library
ii gir1.2-udisks-2.0 2.8.4-1ubuntu1 amd64 GObject based library to access udisks2 - introspection data
ii gir1.2-unity-5.0 7.1.4+19.04.20190319-0ubuntu3 amd64 GObject introspection data for the Unity library
ii gir1.2-upowerlib-1.0 0.99.11-1build2 amd64 GObject introspection data for upower
ii gir1.2-vte-2.91 0.60.3-0ubuntu1~20.04 amd64 GObject introspection data for the VTE library
ii gir1.2-webkit2-4.0 2.28.3-0ubuntu0.20.04.1 amd64 Web content engine library for GTK - GObject introspection data
ii gir1.2-wnck-3.0 3.36.0-1 amd64 GObject introspection data for the WNCK library
ii gjs 1.64.3-1~ubuntu20.04.1 amd64 Mozilla-based javascript bindings for the GNOME platform
ii gkbd-capplet 3.26.1-1 amd64 GNOME control center tools for libgnomekbd
ii glib-networking 2.64.2-1ubuntu0.1 amd64 network-related giomodules for GLib
ii glib-networking-common 2.64.2-1ubuntu0.1 all network-related giomodules for GLib - data files
ii glib-networking-services 2.64.2-1ubuntu0.1 amd64 network-related giomodules for GLib - D-Bus services
ii gnome-accessibility-themes 3.28-1ubuntu1 all High Contrast GTK+ 2 theme and icons
ii gnome-bluetooth 3.34.1-1 amd64 GNOME Bluetooth tools
ii gnome-calculator 1:3.36.0-1ubuntu1 amd64 GNOME desktop calculator
ii gnome-calendar 3.36.2-0ubuntu1 amd64 Calendar application for GNOME
ii gnome-characters 3.34.0-1 amd64 character map application
ii gnome-control-center 1:3.36.4-0ubuntu1 amd64 utilities to configure the GNOME desktop
ii gnome-control-center-data 1:3.36.4-0ubuntu1 all configuration applets for GNOME - data files
ii gnome-control-center-faces 1:3.36.4-0ubuntu1 all utilities to configure the GNOME desktop - faces images
ii gnome-desktop3-data 3.36.3.1-0ubuntu1 all Common files for GNOME desktop apps
ii gnome-disk-utility 3.36.1-1ubuntu1 amd64 manage and configure disk drives and media
ii gnome-font-viewer 3.34.0-2 amd64 font viewer for GNOME
ii gnome-getting-started-docs 3.36.2-0ubuntu0.1 all Help a new user get started in GNOME
ii gnome-getting-started-docs-de 3.36.2-0ubuntu0.1 all Help a new user get started in GNOME (German)
ii gnome-initial-setup 3.36.2-0ubuntu1 amd64 Initial GNOME system setup helper
ii gnome-keyring 3.36.0-1ubuntu1 amd64 GNOME keyring services (daemon and tools)
ii gnome-keyring-pkcs11 3.36.0-1ubuntu1 amd64 GNOME keyring module for the PKCS#11 module loading library
ii gnome-logs 3.34.0-1ubuntu1 amd64 viewer for the systemd journal
ii gnome-mahjongg 1:3.36.1-1 amd64 classic Eastern tile game for GNOME
ii gnome-menus 3.36.0-1ubuntu1 amd64 GNOME implementation of the freedesktop menu specification
ii gnome-mines 1:3.36.0-1 amd64 popular minesweeper puzzle game for GNOME
ii gnome-online-accounts 3.36.0-1ubuntu1 amd64 service to manage online accounts for the GNOME desktop
ii gnome-power-manager 3.32.0-2 amd64 power management tool for the GNOME desktop
ii gnome-screenshot 3.36.0-1ubuntu1 amd64 screenshot application for GNOME
ii gnome-session-bin 3.36.0-2ubuntu1 amd64 GNOME Session Manager - Minimal runtime
ii gnome-session-canberra 0.30-7ubuntu1 amd64 GNOME session log in and log out sound events
ii gnome-session-common 3.36.0-2ubuntu1 all GNOME Session Manager - common files
ii gnome-settings-daemon 3.36.1-0ubuntu1 amd64 daemon handling the GNOME session settings
ii gnome-settings-daemon-common 3.36.1-0ubuntu1 all daemon handling the GNOME session settings - common files
ii gnome-shell 3.36.3-1ubuntu1~20.04.2 amd64 graphical shell for the GNOME desktop
ii gnome-shell-common 3.36.3-1ubuntu1~20.04.2 all common files for the GNOME graphical shell
ii gnome-shell-extension-appindicator 33-1 all AppIndicator/KStatusNotifierItem support for GNOME Shell
ii gnome-shell-extension-desktop-icons 20.04.0-2ubuntu20.04.1 all desktop icon support for GNOME Shell
ii gnome-shell-extension-ubuntu-dock 68ubuntu1~20.04.1 all Ubuntu Dock for GNOME Shell
ii gnome-startup-applications 3.36.0-2ubuntu1 amd64 Startup Applications manager for GNOME
ii gnome-sudoku 1:3.36.0-1 amd64 Sudoku puzzle game for GNOME
ii gnome-system-monitor 3.36.0-1 amd64 Process viewer and system resource monitor for GNOME
ii gnome-terminal 3.36.2-1ubuntu1~20.04 amd64 GNOME terminal emulator application
ii gnome-terminal-data 3.36.2-1ubuntu1~20.04 all Data files for the GNOME terminal emulator
ii gnome-themes-extra 3.28-1ubuntu1 amd64 Adwaita GTK+ 2 theme - engine
ii gnome-themes-extra-data 3.28-1ubuntu1 all Adwaita GTK+ 2 theme - common files
ii gnome-todo 3.28.1-5 amd64 minimalist personal task manager designed to fit GNOME desktop
ii gnome-todo-common 3.28.1-5 all common files for GNOME To Do
ii gnome-user-docs 3.36.2+git20200704-0ubuntu0.1 all GNOME user docs
ii gnome-user-docs-de 3.36.2+git20200704-0ubuntu0.1 all GNOME user docs (German)
ii gnome-video-effects 0.5.0-1ubuntu1 all Collection of GStreamer effects
ii gnupg 2.2.19-3ubuntu2 all GNU privacy guard - a free PGP replacement
ii gnupg-l10n 2.2.19-3ubuntu2 all GNU privacy guard - localization files
ii gnupg-utils 2.2.19-3ubuntu2 amd64 GNU privacy guard - utility programs
ii gpg 2.2.19-3ubuntu2 amd64 GNU Privacy Guard -- minimalist public key operations
ii gpg-agent 2.2.19-3ubuntu2 amd64 GNU privacy guard - cryptographic agent
ii gpg-wks-client 2.2.19-3ubuntu2 amd64 GNU privacy guard - Web Key Service client
ii gpg-wks-server 2.2.19-3ubuntu2 amd64 GNU privacy guard - Web Key Service server
ii gpgconf 2.2.19-3ubuntu2 amd64 GNU privacy guard - core configuration utilities
ii gpgsm 2.2.19-3ubuntu2 amd64 GNU privacy guard - S/MIME version
ii gpgv 2.2.19-3ubuntu2 amd64 GNU privacy guard - signature verification tool
ii grep 3.4-1 amd64 GNU grep, egrep and fgrep
ii grilo-plugins-0.3-base 0.3.11-1ubuntu1 amd64 Framework for discovering and browsing media - Plugins
ii groff-base 1.22.4-4build1 amd64 GNU troff text-formatting system (base system components)
ii grub-common 2.04-1ubuntu26 amd64 GRand Unified Bootloader (common files)
ii grub-grayload-lists 0.7 amd64 GRUB gfxpayload blacklist
ii grub-pc 2.04-1ubuntu26 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 2.04-1ubuntu26 amd64 GRand Unified Bootloader, version 2 (PC/BIOS modules)
ii grub2-common 2.04-1ubuntu26 amd64 GRand Unified Bootloader (common files for version 2)
ii gsettings-desktop-schemas 3.36.0-1ubuntu1 all GSettings desktop-wide schemas
ii gsettings-ubuntu-schemas 0.0.7+17.10.20170922-0ubuntu1 all GSettings desktop-wide schemas for Ubuntu
ii gstreamer1.0-alsa 1.16.2-4 amd64 GStreamer plugin for ALSA
ii gstreamer1.0-clutter-3.0 3.0.27-1 amd64 Clutter Plugin for GStreamer 1.0
ii gstreamer1.0-glx 1.16.2-4 amd64 GStreamer plugins for GL
ii gstreamer1.0-gtk3 1.16.2-1ubuntu2 amd64 GStreamer plugin for GTK+
ii gstreamer1.0-packagekit 1.1.13-2ubuntu1 amd64 GStreamer plugin to install codecs using PackageKit
ii gstreamer1.0-plugins-base 1.16.2-4 amd64 GStreamer plugins from the "base" set
ii gstreamer1.0-plugins-base-apps 1.16.2-4 amd64 GStreamer helper programs from the "base" set
ii gstreamer1.0-plugins-good 1.16.2-1ubuntu2 amd64 GStreamer plugins from the "good" set
ii gstreamer1.0-pulseaudio 1.16.2-1ubuntu2 amd64 GStreamer plugin for PulseAudio
ii gstreamer1.0-tools 1.16.2-2 amd64 Tools for use with GStreamer
ii gstreamer1.0-x 1.16.2-4 amd64 GStreamer plugins for X11 and Pango
ii gtk-update-icon-cache 3.24.20-0ubuntu1 amd64 icon theme caching utility
ii gtk2-engines-murrine 0.98.2-3 amd64 cairo-based gtk+-2.0 theme engine
ii gtk2-engines-pixbuf 2.24.32-4ubuntu4 amd64 pixbuf-based theme for GTK 2
ii guile-2.2-langs 2.2.7+1-4 amd64 Core Guile libraries
ii gvfs 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - GIO module
ii gvfs-backends 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - backends
ii gvfs-bin 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - deprecated command-line tools
ii gvfs-common 1.44.1-1ubuntu1 all userspace virtual filesystem - common data files
ii gvfs-daemons 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - servers
ii gvfs-fuse 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - fuse server

```

```

ii gvfs-libs 1.44.1-1ubuntu1 amd64 userspace virtual filesystem - private libraries
ii gzip 1.10-0ubuntu4 amd64 GNU compression utilities
ii hdparm 9.58+ds-4 amd64 tune hard disk parameters for high performance
ii hicolor-icon-theme 0.17-2 all default fallback theme for FreeDesktop.org icon themes
ii hostname 3.23 amd64 utility to set/show the host name or domain name
ii hplip 3.20.3+dfsg0-2 amd64 HP Linux Printing and Imaging System (HPLIP)
ii hplip-data 3.20.3+dfsg0-2 all HP Linux Printing and Imaging - data files
ii humanity-icon-theme 0.6.15 all Humanity Icon theme
ii hunspell-de-at-frami 1:6.4.3-1 all German (Austria) dictionary for hunspell ("frami" version)
ii hunspell-de-ch-frami 1:6.4.3-1 all German (Switzerland) dictionary for hunspell ("frami" version)
ii hunspell-de-de-frami 1:6.4.3-1 all German dictionary for hunspell ("frami" version)
ii hunspell-en-au 1:2018.04.16-1 all English (Australia) dictionary for hunspell
ii hunspell-en-ca 1:2018.04.16-1 all English (Canada) dictionary for hunspell
ii hunspell-en-gb 1:6.4.3-1 all English (GB) dictionary for hunspell
ii hunspell-en-us 1:2018.04.16-1 all English_american dictionary for hunspell
ii hunspell-en-za 1:6.4.3-1 all English (South Africa) dictionary for hunspell
ii hyphen-de 1:6.4.3-1 all German hyphenation patterns
ii hyphen-en-ca 0.10 all English (Canada) hyphenation patterns
ii hyphen-en-gb 1:6.4.3-1 all English (GB) hyphenation patterns
ii hyphen-en-us 2.8.8-7 all English (US) hyphenation patterns
ii ibus 1.5.22-2ubuntu2.1 amd64 Intelligent Input Bus - core
ii ibus-data 1.5.22-2ubuntu2.1 all Intelligent Input Bus - data files
ii ibus-gtk 1.5.22-2ubuntu2.1 amd64 Intelligent Input Bus - GTK2 support
ii ibus-gtk3 1.5.22-2ubuntu2.1 amd64 Intelligent Input Bus - GTK3 support
ii ibus-table 1.9.25-1 all table engine for IBus
ii libverbs-providers 28.0-1ubuntu1 amd64 User space provider drivers for libibverbs
ii iio-sensor-proxy 2.8-1 amd64 IIO sensors to D-Bus proxy
ii im-config 0.44-1ubuntu1 all Input method configuration framework
ii info 6.7.0.dfsg.2-5 amd64 Standalone GNU Info documentation browser
ii init 1.57 amd64 metapackage ensuring an init system is installed
ii init-system-helpers 1.57 all helper tools for all init systems
ii initramfs-tools 0.136ubuntu6.2 all generic modular initramfs generator (automation)
ii initramfs-tools-bin 0.136ubuntu6.2 amd64 binaries used by initramfs-tools
ii initramfs-tools-core 0.136ubuntu6.2 all generic modular initramfs generator (core tools)
ii inputattach 1:1.7.0-1 amd64 utility to connect serial-attached peripherals to the input subsystem
ii install-info 6.7.0.dfsg.2-5 amd64 Manage installed documentation in info format
ii intel-microcode 3.20200609.0ubuntu0.20.04.2 amd64 Processor microcode firmware for Intel CPUs
ii intltool-debian 0.35.0+20060710.5 all Help i18n of RFC822 compliant config files
ii ippusbxd 1.34-2ubuntu1 amd64 Daemon for IPP USB printer support
ii iproute2 5.5.0-1ubuntu1 amd64 networking and traffic control tools
ii iptables 1.8.4-3ubuntu2 amd64 administration tools for packet filtering and NAT
ii iputils-ping 3:20190709-3 amd64 Tools to test the reachability of network hosts
ii iputils-tracepath 3:20190709-3 amd64 Tools to trace the network path to a remote host
ii irqbalance 1.6.0-3ubuntu1 amd64 Daemon to balance interrupts for SMP systems
ii isc-dhcp-client 4.4.1-2.1ubuntu5 amd64 DHCP client for automatically obtaining an IP address
ii isc-dhcp-common 4.4.1-2.1ubuntu5 amd64 common manpages relevant to all of the isc-dhcp packages
ii iso-codes 4.4-1 all ISO language, territory, currency, script codes and their translations
ii iucode-tool 2.3.1-1 amd64 Intel processor microcode tool
ii iw 5.4-1 amd64 tool for configuring Linux wireless devices
ii kbd 2.0.4-4ubuntu2 amd64 Linux console font and keytable utilities
ii kerneloops 0.12+git20140509-6ubuntu2 amd64 kernel oops tracker
ii keyboard-configuration 1.194ubuntu3 all system-wide keyboard preferences
ii klibc-utils 2.0.7-1ubuntu5 amd64 small utilities built with klibc for early boot
ii kmod 27-lubuntu2 amd64 tools for managing Linux kernel modules
ii krb5-locales 1.17-6ubuntu4 all internationalization support for MIT Kerberos
ii language-pack-de 1:20.04+20200709 all translation updates for language German
ii language-pack-de-base 1:20.04+20200709 all translations for language German
ii language-pack-en 1:20.04+20200709 all translation updates for language English
ii language-pack-en-base 1:20.04+20200709 all translations for language English
ii language-pack-gnome-de 1:20.04+20200709 all GNOME translation updates for language German
ii language-pack-gnome-de-base 1:20.04+20200709 all GNOME translations for language German
ii language-pack-gnome-en 1:20.04+20200709 all GNOME translation updates for language English
ii language-pack-gnome-en-base 1:20.04+20200709 all GNOME translations for language English
ii language-pack-gnome-nds 1:17.10+20171012 all GNOME translation updates for language German, Low
ii language-pack-gnome-nds-base 1:17.10+20171012 all GNOME translations for language German, Low
ii language-pack-nds 1:17.10+20171012 all translation updates for language German, Low
ii language-pack-nds-base 1:17.10+20171012 all translations for language German, Low
ii language-selector-common 0.204 all Language selector for Ubuntu
ii language-selector-gnome 0.204 all Language selector for Ubuntu
ii laptop-detect 0.16 all system chassis type checker
ii less 551-1ubuntu0.1 amd64 pager program similar to more
ii libaai 1.4p5-46 amd64 ASCII art library
ii libabw-0.1-1 0.1.3-1build1 amd64 library for reading and writing AbiWord(tm) documents
ii libaccountsservice0 0.6.55-0ubuntu12-20.04.1 amd64 query and manipulate user account information - shared libraries
ii libacl1 2.2.53-6 amd64 access control list - shared library
ii libai01 0.3.112-5 amd64 Linux kernel AIO access library - shared library
ii libalgorithm-diff-perl 1.19.03-2 all module to find differences between files
ii libalgorithm-diff-xs-perl 0.04-6 amd64 module to find differences between files (XS accelerated)
ii libalgorithm-merge-perl 0.08-3 all Perl module for three-way merge of textual data
ii libamtk-5-0 5.0.2-1build1 amd64 Actions, Menus and Toolbars Kit for GTK+
ii libamtk-5-common 5.0.2-1build1 all Actions, Menus and Toolbars Kit for GTK+ - architecture-independent files
ii libao-common 1.2.2+20180113-1ubuntu1 all Cross Platform Audio Output Library (Common files)
ii libao4 1.2.2+20180113-1ubuntu1 amd64 Cross Platform Audio Output Library
ii libapache2-mod-php7.1 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapache2-mod-php7.2 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapparmor1 2.13.3-7ubuntu5.1 amd64 changehat AppArmor library
ii libappindicator3-1 12.10.1+20.04.20200408.1-0ubuntu1 amd64 Application Indicators
ii libpIRSTream4 0.12.10-2 amd64 Library to access AppStream services
ii libapr1 1.6.5-1ubuntu1 amd64 Apache Portable Runtime Library
ii libaprutil1 1.6.1-4ubuntu2 amd64 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.6.1-4ubuntu2 amd64 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.6.1-4ubuntu2 amd64 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-pkg6.0 2.0.2ubuntu0.1 amd64 package management runtime library
ii libarchive-cpio-perl 0.10-1 all module for manipulations of cpio archives
ii libarchive-zip-perl 1.67-2 all Perl module for manipulation of ZIP archives
ii libarchive13 3.4.0-2ubuntu1 amd64 Multi-format archive and compression library (shared library)
ii libargon2-1 0~20171227.0.2 amd64 memory-hard hashing function - runtime library
ii libasan5 9.3.0-10ubuntu2 amd64 AddressSanitizer -- a fast memory error detector

```

```

ii libasn1-8-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - ASN.1 library
ii libasound2 1.2.2-2.1ubuntu1 amd64 shared library for ALSA applications
ii libasound2-data 1.2.2-2.1ubuntu1 all Configuration files and profiles for ALSA drivers
ii libasound2-plugins 1.2.2-1ubuntu1 amd64 ALSA library additional plugins
ii libaspell15 0.60.8-1build1 amd64 GNU Aspell spell-checker runtime library
ii libassuan0 2.5.3-7ubuntu2 amd64 IPC library for the GnuPG components
ii libasyncns0 0.8-6 amd64 Asynchronous name service query library
ii libatasmart4 0.19-5 amd64 ATA S.M.A.R.T. reading and parsing library
ii libatk-adaptor 2.34.2-0ubuntu2~20.04.1 amd64 AT-SPI 2 toolkit bridge
ii libatk-bridge2.0-0 2.34.2-0ubuntu2~20.04.1 amd64 AT-SPI 2 toolkit bridge - shared library
ii libatk1.0-0 2.35.1-1ubuntu2 amd64 ATK accessibility toolkit
ii libatk1.0-data 2.35.1-1ubuntu2 all Common files for the ATK accessibility toolkit
ii libatkmm-1.6-1v5 2.28.0-2build1 amd64 C++ wrappers for ATK accessibility toolkit (shared libraries)
ii libatm1 1:2.5.1-4 amd64 shared library for ATM (Asynchronous Transfer Mode)
ii libatomic1 10-20200411-0ubuntu1 amd64 support library providing __atomic built-in functions
ii libatopology2 1.2.2-2.1ubuntu1 amd64 shared library for handling ALSA topology definitions
ii libatspi2.0-0 2.36.0-2 amd64 Assistive Technology Service Provider Interface - shared library
ii libattr1 1:2.4.48-5 amd64 extended attribute handling - shared library
ii libaudit-common 1:2.8.5-2ubuntu6 all Dynamic library for security auditing - common files
ii libaudit1 1:2.8.5-2ubuntu6 amd64 Dynamic library for security auditing
ii libauthen-sasl-perl 2.1600-1 all Authen::SASL - SASL Authentication framework
ii libavahi-client3 0.7-4ubuntu7 amd64 Avahi Client library
ii libavahi-common-data 0.7-4ubuntu7 amd64 Avahi common data files
ii libavahi-common3 0.7-4ubuntu7 amd64 Avahi common library
ii libavahi-core7 0.7-4ubuntu7 amd64 Avahi's embeddable mDNS/DNS-SD library
ii libavahi-glib1 0.7-4ubuntu7 amd64 Avahi GLib integration library
ii libavahi-ui-gtk3-0 0.7-4ubuntu7 amd64 Avahi GTK+ User interface library for GTK3
ii libavc1394-0 0.5.4-5 amd64 control IEEE 1394 audio/video devices
ii libbbeltrace1 1.5.8-1build1 amd64 Babeltrace conversion libraries
ii libbinutils 2.34-6ubuntu1 amd64 GNU binary utilities (private shared library)
ii libblkid1 2.34-0.1ubuntu9 amd64 block device ID library
ii libblockdev-crypto2 2.23-2ubuntu3 amd64 Crypto plugin for libblockdev
ii libblockdev-fs2 2.23-2ubuntu3 amd64 file system plugin for libblockdev
ii libblockdev-loop2 2.23-2ubuntu3 amd64 Loop device plugin for libblockdev
ii libblockdev-part-err2 2.23-2ubuntu3 amd64 Partition error utility functions for libblockdev
ii libblockdev-part2 2.23-2ubuntu3 amd64 Partitioning plugin for libblockdev
ii libblockdev-swap2 2.23-2ubuntu3 amd64 Swap plugin for libblockdev
ii libblockdev-utils2 2.23-2ubuntu3 amd64 Utility functions for libblockdev
ii libblockdev2 2.23-2ubuntu3 amd64 Library for manipulating block devices
ii libbluetooth3 5.53-0ubuntu3 amd64 Library to use the BlueZ Linux Bluetooth stack
ii libboost-date-time1.71.0 1.71.0-6ubuntu6 amd64 set of date-time libraries based on generic programming concepts
ii libboost-filesystem1.71.0 1.71.0-6ubuntu6 amd64 filesystem operations (portable paths, iteration over directories, etc) in C++
ii libboost-iostreams1.71.0 1.71.0-6ubuntu6 amd64 Boost.Iostreams Library
ii libboost-locale1.71.0 1.71.0-6ubuntu6 amd64 C++ facilities for localization
ii libboost-thread1.71.0 1.71.0-6ubuntu6 amd64 portable C++ multi-threading
ii libbrlapi0.7 6.0+dfsg-4ubuntu6 amd64 braille display access via BRLTTY - shared library
ii libbrotli1 1.0.7-6build1 amd64 library implementing brotli encoder and decoder (shared libraries)
ii libbsd0 0.10.0-1 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.8-2 amd64 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.31-0ubuntu9 amd64 GNU C Library: Binaries
ii libc-dev-bin 2.31-0ubuntu9 amd64 GNU C Library: Development binaries
ii libc6 2.31-0ubuntu9 amd64 GNU C Library: Shared libraries
ii libc6-dbg 2.31-0ubuntu9 amd64 GNU C Library: detached debugging symbols
ii libc6-dev 2.31-0ubuntu9 amd64 GNU C Library: Development Libraries and Header Files
ii libcaca0 0.99.beta19-2.1ubuntu1 amd64 colour ASCII art library
ii libcairo-gobject-perl 1.005-2 amd64 integrate Cairo into the Glib type system in Perl
ii libcairo-gobject2 1.16.0-4ubuntu1 amd64 Cairo 2D vector graphics library (GObject library)
ii libcairo-perl 1.107-1 amd64 Perl interface to the Cairo graphics library
ii libcairo2 1.16.0-4ubuntu1 amd64 Cairo 2D vector graphics library
ii libcairomm-1.0-1v5 1.12.2-4build1 amd64 C++ wrappers for Cairo (shared libraries)
ii libcamel-1.2-62 3.36.3-0ubuntu1.1 amd64 Evolution MIME message handling library
ii libcanberra-gtk3-0 0.30-7ubuntu1 amd64 GTK+ 3.0 helper for playing widget event sounds with libcanberra
ii libcanberra-gtk3-module 0.30-7ubuntu1 amd64 translates GTK3 widgets signals to event sounds
ii libcanberra-pulse 0.30-7ubuntu1 amd64 PulseAudio backend for libcanberra
ii libcanberra0 0.30-7ubuntu1 amd64 simple abstract interface for playing event sounds
ii libcap-ng0 0.7.9-2.1build1 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.32-1 amd64 POSIX 1003.1e capabilities (library)
ii libcap2-bin 1:2.32-1 amd64 POSIX 1003.1e capabilities (utilities)
ii libcbor0.6 0.6.0-0ubuntu1 amd64 library for parsing and generating CBOR (RFC 7049)
ii libcc1-0 10-20200411-0ubuntu1 amd64 GCC cc1 plugin for GDB
ii libcdio-cdda2 10.2+2.0.0-1 amd64 library to read and control digital audio CDs
ii libcdio-paranoia2 10.2+2.0.0-1 amd64 library to read digital audio CDs with error correction
ii libcdio18 2.0.0-2 amd64 library to read and control CD-ROM
ii libcdparanoia0 3.10.2+debian-13 amd64 audio extraction tool for sampling CDs (library)
ii libcdr-0.1-1 0.1.6-1build2 amd64 library for reading and converting Corel DRAW files
ii libcephfs2 15.2.3-0ubuntu0.20.04.1 amd64 Ceph distributed file system client library
ii libcgi-fast-perl 1:2.15-1 all CGI subclass for work with FCGI
ii libcgi-pm-perl 4.46-1 all module for Common Gateway Interface applications
ii libcheese-gtk25 3.34.0-1build1 amd64 tool to take pictures and videos from your webcam - widgets
ii libcheese8 3.34.0-1build1 amd64 tool to take pictures and videos from your webcam - base library
ii libclucene-contribs1v5 2.3.3.4+dfsg-1build1 amd64 language specific text analyzers (runtime)
ii libclucene-core1v5 2.3.3.4+dfsg-1build1 amd64 core library for full-featured text search engine (runtime)
ii libclutter-1.0-0 1.26.4+dfsg-1 amd64 Open GL based interactive canvas library
ii libclutter-1.0-common 1.26.4+dfsg-1 all Open GL based interactive canvas library (common files)
ii libclutter-gst-3.0-0 3.0.27-1 amd64 Open GL based interactive canvas library GStreamer elements
ii libclutter-gtk-1.0-0 1.8.4-4 amd64 Open GL based interactive canvas library GTK+ widget
ii libcmis-0.5-5v5 0.5.2-1ubuntu1 amd64 CMIS protocol client library
ii libcogl-common 1.22.6-1 all Object oriented GL/GLES Abstraction/Utility Layer (common files)
ii libcogl-pango20 1.22.6-1 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl-path20 1.22.6-1 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl120 1.22.6-1 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcolamd2 1:5.7.1+dfsg-2 amd64 column approximate minimum degree ordering library for sparse matrices
ii libcolord-gtk1 0.2.0-0ubuntu1 amd64 GTK+ convenience library for interacting with colord
ii libcolord2 1.4.4-2 amd64 system service to manage device colour profiles -- runtime
ii libcolorhug2 1.4.4-2 amd64 library to access the ColorHug colourimeter -- runtime
ii libcom-err2 1.45.5-2ubuntu1 amd64 common error description library
ii libconfig-inifiles-perl 3.00002-1 all read .ini-style configuration files
ii libcrack2 2.9.6-3.2 amd64 pro-active password checker library
ii libcroco3 0.6.13-1 amd64 Cascading Style Sheet (CSS) parsing and manipulation toolkit

```

```

ii libcrypt-dev 1:4.4.10-10ubuntu4 amd64 libcrypt development files
ii libcrypt1 1:4.4.10-10ubuntu4 amd64 libcrypt shared library
ii libcryptsetup12 2:2.2.2-3ubuntu2 amd64 disk encryption support - shared library
ii libctf-nobfd0 2.34-6ubuntu1 amd64 Compact C Type Format library (runtime, no BFD dependency)
ii libctf0 2.34-6ubuntu1 amd64 Compact C Type Format library (runtime, BFD dependency)
ii libcue2 2.2.1-2 amd64 CUE Sheet Parser Library
ii libcurls2 2.3.1-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - Core library
ii libcurlsfilters1 1.27.4-1 amd64 OpenPrinting CUPS Filters - Shared library
ii libcurlsimage2 2.31.9-9ubuntu1.1 amd64 Common UNIX Printing System(tm) - Raster image library
ii libcurls-gnutls 7.68.0-1ubuntu2.1 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libcurl4 7.68.0-1ubuntu2.1 amd64 easy-to-use client-side URL transfer library (OpenSSL flavour)
ii libdaemon0 0.14-7 amd64 lightweight C library for daemons - runtime library
ii libdump-perl 1.23-1 all Perl module to help dump data structures
ii libdatrie1 0.2.12-3 amd64 Double-array trie library
ii libdazzle-1.0-0 3.36.0-1 amd64 feature-filled library for GTK+ and GObject
ii libdb5.3 5.3.28+dfsg1-0.6ubuntu2 amd64 Berkeley v5.3 Database Libraries [runtime]
ii libdbd-mysql-perl 4.050-3 amd64 Perl5 database interface to the MariaDB/MySQL database
ii libdbi-perl 1.643-1 amd64 Perl Database Interface (DBI)
ii libdbus-1-3 1.12.16-2ubuntu2.1 amd64 simple interprocess messaging system (library)
ii libdbus-glib-1-2 0.110-5fakssync1 amd64 deprecated library for D-Bus IPC
ii libibusmenu-glib4 16.04.1+18.10.20180917-0ubuntu6 amd64 library for passing menus over DBus
ii libibusmenu-gtk3-4 16.04.1+18.10.20180917-0ubuntu6 amd64 library for passing menus over DBus - GTK+ version
ii libdconf1 0.36.0-1 amd64 simple configuration storage system - runtime library
ii libdebcfgclient0 0.251ubuntu1 amd64 Debian Configuration Management System (C-implementation library)
ii libdebhelper-perl 12.10ubuntu1 all debhelper perl modules
ii libdee-1.0-4 1.2.7+17.10.20170616-4ubuntu6 amd64 Model to synchronize multiple instances over DBus - shared lib
ii libdevmapper1.02.1 2:1.02.167-1ubuntu1 amd64 Linux Kernel Device Mapper userspace library
ii libdjvulibre-text 3.5.27.1-14build1 all Linguistic support files for libdjvulibre
ii libdjvulibre21 3.5.27.1-14build1 amd64 Runtime support for the DjVu image format
ii libdmapharing-3.0-2 2.9.39-6 amd64 DMAP client and server library - runtime
ii libdns-export1109 1:9.11.16+dfsg-3~build1 amd64 Exported DNS Shared Library
ii libdotconf0 1.3-0.3fakesync1 amd64 Configuration file parser library - runtime files
ii libdpkg-perl 1.19.7ubuntu3 all Dpkg perl modules
ii libdrm-amdgpu1 2.4.101-2 amd64 Userspace interface to amdgpu-specific kernel DRM services -- runtime
ii libdrm-common 2.4.101-2 all Userspace interface to kernel DRM services -- common files
ii libdrm-intel1 2.4.101-2 amd64 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau2 2.4.101-2 amd64 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.101-2 amd64 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.101-2 amd64 Userspace interface to kernel DRM services -- runtime
ii libdv4 1.0.0-12 amd64 software library for DV format digital video (runtime lib)
ii libdw1 0.176-1.1build1 amd64 library that provides access to the DWARF debug information
ii libe-book-0.1-1 0.1.3-1build3 amd64 library for reading and converting various e-book formats
ii libebackend-1.2-10 3.36.3-0ubuntu1.1 amd64 Utility library for evolution data servers
ii libebook-1.2-20 3.36.3-0ubuntu1.1 amd64 Client library for evolution address books
ii libebook-contacts-1.2-3 3.36.3-0ubuntu1.1 amd64 Client library for evolution contacts books
ii libecal-2.0-1 3.36.3-0ubuntu1.1 amd64 Client library for evolution calendars
ii libedata-book-1.2-26 3.36.3-0ubuntu1.1 amd64 Backend library for evolution address books
ii libedata-cal-2.0-1 3.36.3-0ubuntu1.1 amd64 Backend library for evolution calendars
ii libedataserver-1.2-24 3.36.3-0ubuntu1.1 amd64 Utility library for evolution data servers
ii libedataserverui-1.2-2 3.36.3-0ubuntu1.1 amd64 Utility library for evolution data servers
ii libedit2 3.1-20191231-1 amd64 BSD editline and history libraries
ii libefiboot1 37-2ubuntu2 amd64 Library to manage UEFI variables
ii libefivar1 37-2ubuntu2 amd64 Library to manage UEFI variables
ii libegl-mesa0 20.0.8-0ubuntu1~20.04.1 amd64 free implementation of the EGL API -- Mesa vendor library
ii libegl1 1.3.1-1 amd64 Vendor neutral GL dispatch library -- EGL support
ii libelf1 0.176-1.1build1 amd64 library to read and write ELF files
ii libenchant-2-2 2.2.8-1 amd64 Wrapper library for various spell checker engines (runtime libs)
ii libencode-locale-perl 1.05-1 all utility to determine the locale encoding
ii libeot0 0.01-5 amd64 Library for parsing/converting Embedded OpenType files
ii libepoxy0 1.5.4-1 amd64 OpenGL function pointer management library
ii libepubgen-0.1-1 0.1.1-1ubuntu2 amd64 EPUB generator library
ii libespeak-ng1 1.50+dfsg-6 amd64 Multi-lingual software speech synthesizer: shared library
ii libestr0 0.1.10-2.1 amd64 Helper functions for handling strings (lib)
ii libetonyek-0.1-1 0.1.9-3 amd64 library for reading and converting Apple Keynote presentations
ii libevdev2 1.9.0+dfsg-1 amd64 wrapper library for evdev devices
ii libevdocument3-4 3.36.7-0ubuntu1 amd64 Document (PostScript, PDF) rendering library
ii libevent-2.1-7 2.1.11-stable-1 amd64 Asynchronous event notification library
ii libevview3-3 3.36.7-0ubuntu1 amd64 Document (PostScript, PDF) rendering library - Gtk+ widgets
ii libexempi8 2.5.1-1build1 amd64 library to parse XMP metadata (Library)
ii libexif12 0.6.21-6ubuntu0.3 amd64 library to parse EXIF files
ii libexiv2-27 0.27.2-8ubuntu2 amd64 EXIF/IPTC/XMP metadata manipulation library
ii libexpat1 2.2.9-1build1 amd64 XML parsing C library - runtime library
ii libext2fs2 1.45.5-2ubuntu1 amd64 ext2/ext3/ext4 file system libraries
ii libexttextcat-2.0-0 3.4.5-1 amd64 Language detection library
ii libexttextcat-data 3.4.5-1 all Language detection library - data files
ii libextutils-depends-perl 0.8000-1 all Perl module for building extensions that depend on other extensions
ii libextutils-pkgconfig-perl 1.16-1 all Perl interface to the pkg-config utility
ii libfakeroot 1.24-1 amd64 tool for simulating superuser privileges - shared libraries
ii libfastjson4 0.99.8-2 amd64 fast json library for C
ii libfcgi-perl 0.79-1 amd64 helper module for FastCGI
ii libfdisk1 2.34-0.1ubuntu9 amd64 fdisk partitioning library
ii libffif1 3.3-4 amd64 Foreign Function Interface library runtime
ii libfftw3-single3 3.3.8-2ubuntu1 amd64 Library for computing Fast Fourier Transforms - Single precision
ii libfido2-1 1.3.1-1ubuntu2 amd64 library for generating and verifying FIDO 2.0 objects
ii libfile-basedir-perl 0.08-1 all Perl module to use the freedesktop basedir specification
ii libfile-desktopentry-perl 0.22-1 all Perl module to handle freedesktop .desktop files
ii libfile-fcntllock-perl 0.22-3build4 amd64 Perl module for file locking with fcntl(2)
ii libfile-listing-perl 6.04-1 all module to parse directory listings
ii libfile-mimeinfo-perl 0.29-1 all Perl module to determine file types
ii libfile-stripndeterminism-perl 1.7.0-1 all file non-deterministic information stripper - Perl module
ii libflac8 1.3.3-1build1 amd64 Free Lossless Audio Codec - runtime C library
ii libfont-afm-perl 1.20-2 all Font::AFM - Interface to Adobe Font Metrics files
ii libfontconfig1 2.13.1-2ubuntu3 amd64 generic font configuration library - runtime
ii libfontembed1 1.27.4-1 amd64 OpenPrinting CUPS Filters - Font Embed Shared library
ii libfontenc1 1:1.1.4-0ubuntu1 amd64 X11 font encoding library
ii libfpprint-2-2 1:1.1.90.1+tod1-0ubuntu4 amd64 async fingerprint library of fpprint project, shared libraries
ii libfpprint-2-tod1 1:1.90.1+tod1-0ubuntu4 amd64 async fingerprint library of fpprint project, drivers shared libraries
ii libfreerhand-0.1-1 0.1.2-2ubuntu1 amd64 Library for parsing the FreeHand file format structure
ii libfreerdp-client2-2 2.1.1+dfsg1-0ubuntu0.20.04.1 amd64 Free Remote Desktop Protocol library (client library)

```

```

ii libfreerdp2-2 2.1.1+dfsg1-0ubuntu0.20.04.1 amd64 Free Remote Desktop Protocol library (core library)
ii libfreetype6 2.10.1-2 amd64 FreeType 2 font engine, shared library files
ii libfribidi0 1.0.8-2 amd64 Free Implementation of the Unicode BiDi algorithm
ii libfuse2 2.9.9-3 amd64 Filesystem in Userspace (library)
ii libfwupd2 1.3.11-1~focal1 amd64 Firmware update daemon library
ii libfwupdplugin1 1.3.11-1~focal1 amd64 Firmware update daemon plugin library
ii libgail-common 2.24.32-4ubuntu4 amd64 GNOME Accessibility Implementation Library -- common modules
ii libgail18 2.24.32-4ubuntu4 amd64 GNOME Accessibility Implementation Library -- shared libraries
ii libgamemode0 1.5.1-0ubuntu3.1 amd64 Optimise Linux system performance on demand (libraries)
ii libgamemodeauto0 1.5.1-0ubuntu3.1 amd64 Automatically optimise Linux system performance on demand
ii libgbm1 20.0.8-0ubuntu1~20.04.1 amd64 generic buffer management API -- runtime
ii libgc1c2 1:7.6.4-0.4ubuntu1 amd64 conservative garbage collector for C and C++
ii libgcab-1.0-0 1.4-1 amd64 Microsoft Cabinet file manipulation library
ii libgcc-9-dev 9.3.0-10ubuntu2 amd64 GCC support library (development files)
ii libgcc-s1 10-20200411-0ubuntu1 amd64 GCC support library
ii libgck-1-0 3.36.0-2build1 amd64 Glib wrapper library for PKCS#11 - runtime
ii libgcr-base-3-1 3.36.0-2build1 amd64 Library for Crypto related tasks
ii libgcr-ui-3-1 3.36.0-2build1 amd64 Library for Crypto UI related tasks
ii libgcrypt20 1.8.5-5ubuntu1 amd64 LGPL Crypto library - runtime library
ii libgd3 2.3.0-2+ubuntu20.04.1+deb.sury.org+1 amd64 GD Graphics Library
ii libgdata-common 0.17.12-1 all Library for accessing GData webservices - common data files
ii libgdata22 0.17.12-1 amd64 Library for accessing GData webservices - shared libraries
ii libgdbs-compat4 1.18.1-5 amd64 GNU dbm database routines (legacy support runtime version)
ii libgdbs6 1.18.1-5 amd64 GNU dbm database routines (runtime version)
ii libgdk-pixbuf2.0-0 2.40.0+dfsg-3 amd64 GDK Pixbuf library
ii libgdk-pixbuf2.0-bin 2.40.0+dfsg-3 amd64 GDK Pixbuf library (thumbnailer)
ii libgdk-pixbuf2.0-common 2.40.0+dfsg-3 all GDK Pixbuf library - data files
ii libgdm1 3.34.1-1ubuntu1 amd64 GNOME Display Manager (shared library)
ii libgee-0.8-2 0.20.3-1 amd64 GObject based collection and utility library
ii libgeocircle-2-0 2.5.6-0ubuntu1 amd64 convenience library to interact with geoinformation service
ii libgeocode-glib0 3.26.2-2 amd64 geocoding and reverse geocoding Glib library using Nominatim
ii libgexiv2-2 0.12.0-2 amd64 GObject-based wrapper around the Exiv2 library
ii libgif7 5.1.9-1 amd64 library for GIF images (library)
ii libgirepository-1.0-1 1.64.1-1~ubuntu20.04.1 amd64 Library for handling GObject introspection data (runtime library)
ii libgjs0g 1.64.3-1~ubuntu20.04.1 amd64 Mozilla-based javascript bindings for the GNOME platform
ii libgl1 1.3.1-1 amd64 Vendor neutral GL dispatch library -- legacy GL support
ii libgl1-mesa-dri 20.0.8-0ubuntu1~20.04.1 amd64 free implementation of the OpenGL API -- DRI modules
ii libglapi-mesa 20.0.8-0ubuntu1~20.04.1 amd64 free implementation of the GL API -- shared library
ii libgles2 1.3.1-1 amd64 Vendor neutral GL dispatch library -- GLESv2 support
ii libglib-object-introspection-perl 0.048-2build1 amd64 Perl bindings for gobject-introspection libraries
ii libglib-perl 3:1.329.2-1 amd64 interface to the GLib and GObject libraries
ii libglib2.0-0 2.64.3-1~ubuntu20.04.1 amd64 GLib library of C routines
ii libglib2.0-bin 2.64.3-1~ubuntu20.04.1 amd64 Programs for the GLib library
ii libglib2.0-data 2.64.3-1~ubuntu20.04.1 all Common files for GLib library
ii libglibmm-2.4-1v5 2.64.2-1 amd64 C++ wrapper for the Glib toolkit (shared libraries)
ii libglu1-mesa 9.0.1-1build1 amd64 Mesa OpenGL utility library (GLU)
ii libglvnd0 1.3.1-1 amd64 Vendor neutral GL dispatch library
ii libglx-mesa0 20.0.8-0ubuntu1~20.04.1 amd64 free implementation of the OpenGL API -- GLX vendor library
ii libglx0 1.3.1-1 amd64 Vendor neutral GL dispatch library -- GLX support
ii libgmp10 2:6.2.0+dfsg-4 amd64 Multiprecision arithmetic library
ii libgnome-autoar-0 0.2.3-2 amd64 Archives integration support for GNOME
ii libgnome-bluetooth13 3.34.1-1 amd64 GNOME Bluetooth tools - support library
ii libgnome-desktop-3-19 3.36.3.1-0ubuntu1 amd64 Utility library for loading .desktop files - runtime files
ii libgnome-games-support-1-3 1.6.1-1 amd64 library for common functions of GNOME games
ii libgnome-games-support-common 1.6.1-1 all library for common functions of GNOME games (common files)
ii libgnome-menu-3-0 3.36.0-1ubuntu1 amd64 GNOME implementation of the freedesktop menu specification
ii libgnome-todo 3.28.1-5 amd64 library data for GNOME To Do
ii libgnomekbd-common 3.26.1-1 all GNOME library to manage keyboard configuration - common files
ii libgnomekbd8 3.26.1-1 amd64 GNOME library to manage keyboard configuration - shared library
ii libgnutls30 3.6.13-2ubuntu1.2 amd64 GNU TLS library - main runtime library
ii libgoa-1.0-0b 3.36.0-1ubuntu1 amd64 library for GNOME Online Accounts
ii libgoa-1.0-common 3.36.0-1ubuntu1 all library for GNOME Online Accounts - common files
ii libgoa-backend-1.0-1 3.36.0-1ubuntu1 amd64 backend library for GNOME Online Accounts
ii libgom-1.0-0 0.4-1 amd64 Object mapper from GObjects to SQLite
ii libgomp1 10-20200411-0ubuntu1 amd64 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.37-1 amd64 GnuPG development runtime library
ii libgpgme11 1.13.1-7ubuntu2 amd64 GPGME - GnuPG Made Easy (library)
ii libgpgmepp6 1.13.1-7ubuntu2 amd64 C++ wrapper library for GPGME
ii libgphoto2-6 2.25.25-0ubuntu0.1 amd64 gphoto2 digital camera library
ii libgphoto2-110n 2.25.25-0ubuntu0.1 all gphoto2 digital camera library - localized messages
ii libgphoto2-port12 2.25.25-0ubuntu0.1 amd64 gphoto2 digital camera port library
ii libgpmm 1.20.7-5 amd64 General Purpose Mouse - shared library
ii libgpod-common 0.8.3-15 amd64 common files for libgpod
ii libgraphene-1.0-0 1.10.0-1build2 amd64 library of graphic data types
ii libgraphite2-3 1.3.13-11build1 amd64 Font rendering engine for Complex Scripts -- library
ii libgrilo-0.3-0 0.3.12-1 amd64 Framework for discovering and browsing media - Shared libraries
ii libgs9 9.50~dfsg-5ubuntu4 amd64 interpreter for the PostScript language and for PDF - Library
ii libgs9-common 9.50~dfsg-5ubuntu4 all interpreter for the PostScript language and for PDF - common files
ii libgsf-1-114 1.14.46-1 amd64 Structured File Library - runtime version
ii libgsf-1-common 1.14.46-1 all Structured File Library - common files
ii libgsound0 1.0.2-4 amd64 small library for playing system sounds
ii libgspell-1-2 1.8.3-1 amd64 spell-checking library for GTK+ applications
ii libgspell-1-common 1.8.3-1 all libgspell architecture-independent files
ii libgssapi-krb5-2 1.17.6ubuntu4 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssapi3-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - GSSAPI support library
ii libgssdp-1.2-0 1.2.2-1 amd64 GObject-based library for SSDP
ii libgststreamer-g11-0-0 1.16.2-4 amd64 GStreamer GL libraries
ii libgststreamer-plugins-base1.0-0 1.16.2-4 amd64 GStreamer libraries from the "base" set
ii libgststreamer-plugins-good1.0-0 1.16.2-1ubuntu2 amd64 GStreamer development files for libraries from the "good" set
ii libgststreamer1.0-0 1.16.2-2 amd64 Core GStreamer libraries and elements
ii libgtk-3-0 3.24.20-0ubuntu1 amd64 GTK graphical user interface library
ii libgtk-3-bin 3.24.20-0ubuntu1 amd64 programs for the GTK graphical user interface library
ii libgtk-3-common 3.24.20-0ubuntu1 all common files for the GTK graphical user interface library
ii libgtk2.0-0 2.24.32-4ubuntu4 amd64 GTK graphical user interface library - old version
ii libgtk2.0-bin 2.24.32-4ubuntu4 amd64 programs for the GTK graphical user interface library
ii libgtk2.0-common 2.24.32-4ubuntu4 all common files for the GTK graphical user interface library
ii libgtk3-perl 0.037-1 all Perl bindings for the GTK+ graphical user interface library
ii libgtkmm-3.0-1v5 3.24.2-1build1 amd64 C++ wrappers for GTK+ (shared libraries)

```

```

ii libgtksourceview-4-0 4.6.0-1 amd64 shared libraries for the GTK+ syntax highlighting widget
ii libgtksourceview-4-common 4.6.0-1 all common files for the GTK+ syntax highlighting widget
ii libgtop-2.0-11 2.40.0-2 amd64 gtop system monitoring library (shared)
ii libgtop2-common 2.40.0-2 all gtop system monitoring library (common)
ii libgudev-1.0-0 1:233-1 amd64 GObject-based wrapper library for libudev
ii libgupnp-1.2-0 1.2.2-1 amd64 GObject-based library for UPnP
ii libgupnp-av-1.0-2 0.12.11-2 amd64 Audio/Visual utility library for GUPnP
ii libgupnp-dlna-2.0-3 0.10.5-4 amd64 DLNA utility library for GUPnP
ii libgusb2 0.3.4-0.1 amd64 GLib wrapper around libusb1
ii libgweather-3-16 3.36.0-1 amd64 GWeather shared library
ii libgweather-common 3.36.0-1 all GWeather common files
ii libgxps2 0.3.1-1 amd64 handling and rendering XPS documents (library)
ii libhandy-0.0-0 0.0.13-1 amd64 Library with GTK widgets for mobile phones
ii libharfbuzz-icu0 2.6.4-1ubuntu4 amd64 OpenType text shaping engine ICU backend
ii libharfbuzz0b 2.6.4-1ubuntu4 amd64 OpenType text shaping engine (shared library)
ii libhcrypto4-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - crypto library
ii libheimbase1-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - Base library
ii libheimntlm0-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - NTLM support library
ii libhogweed5 3.5.1+really3.5.1-2 amd64 low level cryptographic library (public-key cryptos)
ii libhpmd0 3.20.3+dfsg0-2 amd64 HP Multi-Point Transport Driver (hpmd) run-time libraries
ii libhtml-form-perl 6.07-1 all module that represents an HTML form element
ii libhtml-format-perl 2.12-1 all module for transforming HTML into various formats
ii libhtml-parser-perl 3.72-5 amd64 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-4 all data tables pertaining to HTML
ii libhtml-template-perl 2.97-1 all module for using HTML templates with Perl
ii libhtml-tree-perl 5.07-2 all Perl module to represent and create HTML syntax trees
ii libhttp-cookies-perl 6.08-1 all HTTP cookie jars
ii libhttp-daemon-perl 6.06-1 all simple http server class
ii libhttp-date-perl 6.05-1 all module of date conversion routines
ii libhttp-message-perl 6.22-1 all perl interface to HTTP style messages
ii libhttp-negotiate-perl 6.01-1 all implementation of content negotiation
ii libhunspell-1.7-0 1.7.0-2build2 amd64 spell checker and morphological analyzer (shared library)
ii libhx509-5-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - X509 support library
ii libhyphen0 2.8.8-7 amd64 ALTlinux hyphenation library - shared library
ii libibus-1.0-5 1.5.22-2ubuntu2.1 amd64 Intelligent Input Bus - shared library
ii libibverbs1 28.0-1ubuntu1 amd64 Library for direct userspace use of RDMA (InfiniBand/iWARP)
ii libical3 3.0.8-1 amd64 iCalendar library implementation in C (runtime)
ii libice6 2:1.0.10-0ubuntu1 amd64 X11 Inter-Client Exchange library
ii libicu66 66.1-2ubuntu2 amd64 International Components for Unicode
ii libidn11 1.33-2.2ubuntu2 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libidn2-0 2.3.0-1+ubuntu20.04.1+deb.sury.org+2 amd64 Internationalized domain names (IDNA2008/TR46) library
ii libiec61883-0 1.2.0-3 amd64 partial implementation of IEC 61883 (shared lib)
ii libieee1284-3 0.2.11-13build1 amd64 cross-platform library for parallel port access
ii libijs-0.35 0.35-15 amd64 IJS raster image transport protocol: shared library
ii libimagequant0 2.12.2-1.1 amd64 palette quantization library
ii libimobiledevice6 1.2.1~git20191129.9f79242-1build1 amd64 Library for communicating with iPhone and other Apple devices
ii libinput-bin 1.15.5-1 amd64 input device management and event handling library - udev quirks
ii libinput10 1.15.5-1 amd64 input device management and event handling library - shared library
ii libio-html-perl 1.001-1 all open an HTML file with automatic charset detection
ii libio-socket-ssl-perl 2.067-1 all Perl module implementing object oriented interface to SSL sockets
ii libio-stringy-perl 2.111-3 all modules for I/O on in-core objects (strings/arrays)
ii libip4tc2 1.8.4-3ubuntu2 amd64 netfilter libip4tc library
ii libip6tc2 1.8.4-3ubuntu2 amd64 netfilter libip6tc library
ii libipc-system-simple-perl 1.26-1 all Perl module to run commands simply, with detailed diagnostics
ii libisc-export1105 1:9.11.16+dfsg-3~build1 amd64 Exported ISC Shared Library
ii libis122 0.22.1-1 amd64 manipulating sets and relations of integer points bounded by linear constraints
ii libitm1 10-20200411-0ubuntu1 amd64 GNU Transactional Memory Library
ii libiw30 30~pre9-13ubuntu1 amd64 Wireless tools - library
ii libjack-jackd2-0 1.9.12~dfsg-2ubuntu2 amd64 JACK Audio Connection Kit (libraries)
ii libjansson4 2.12-1build1 amd64 C library for encoding, decoding and manipulating JSON data
ii libjavascrptcoregtk-4.0-18 2.28.3-0ubuntu0.20.04.1 amd64 JavaScript engine library from WebKitGTK
ii libjbigr0 2.1-3.1build1 amd64 JBIGkit libraries
ii libjbigr2dec0 0.18-1ubuntu1 amd64 JBIG2 decoder library - shared libraries
ii libjpeg-turbo8 2.0.3-0ubuntu1.20.04.1 amd64 IJG JPEG compliant runtime library.
ii libjpeg8 8c-2ubuntu8 amd64 Independent JPEG Group's JPEG runtime library (dependency package)
ii libjson-c4 0.13.1+dfsg-7ubuntu0.3 amd64 JSON manipulation library - shared library
ii libjson-glib-1.0-0 1.4.4-2ubuntu2 amd64 GLib JSON manipulation library
ii libjson-glib-1.0-common 1.4.4-2ubuntu2 all GLib JSON manipulation library (common files)
ii libjuh-java 1:6.4.4-0ubuntu0.20.04.1 all LibreOffice UNO runtime environment -- Java Uno helper
ii libjurt-java 1:6.4.4-0ubuntu0.20.04.1 all LibreOffice UNO runtime environment -- Java Uno Runtime
ii libk5crypto3 1.17-6ubuntu4 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.6-6ubuntu1 amd64 Linux Key Management Utilities (library)
ii libklc2 2.0.7-1ubuntu5 amd64 minimal libc subset for use with initramfs
ii libkmod2 27-1ubuntu2 amd64 libkmod shared library
ii libkpathsea6 2019.20190605.51237-3build2 amd64 TeX Live: path search library for TeX (runtime part)
ii libkrb5-26-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - libraries
ii libkrb5-3 1.17-6ubuntu4 amd64 MIT Kerberos runtime libraries
ii libkrb5support0 1.17-6ubuntu4 amd64 MIT Kerberos runtime libraries - Support library
ii libksba8 1.3.5-2 amd64 X.509 and CMS support library
ii liblangtag-common 0.6.3-1 all library to access tags for identifying languages -- data
ii liblangtag1 0.6.3-1 amd64 library to access tags for identifying languages
ii liblcms2-2 2.9-4 amd64 Little CMS 2 color management library
ii liblcms2-utils 2.9-4 amd64 Little CMS 2 color management library (utilities)
ii libldap-2.4-2 2.4.49+dfsg-2ubuntu1.3 amd64 OpenLDAP libraries
ii libldap-common 2.4.49+dfsg-2ubuntu1.3 all OpenLDAP common files for libraries
ii libldb2 2:2.0.10-0ubuntu0.20.04.1 amd64 LDAP-like embedded database - shared library
ii liblirc-client0 0.10.1-6.1ubuntu1.1 amd64 infra-red remote control support - client library
ii libllvm10 1:10.0.0-4ubuntu1 amd64 Modular compiler and toolchain technologies, runtime library
ii liblvm9 1:9.0.1-12 amd64 Modular compiler and toolchain technologies, runtime library
ii liblmdb0 0.9.24-1 amd64 Lightning Memory-Mapped Database shared library
ii liblocale-gettext-perl 1.07-4 amd64 module using libc functions for internationalization in Perl
ii liblouis-data 3.12.0-3 all Braille translation library - data
ii liblouis20 3.12.0-3 amd64 Braille translation library - shared libs
ii liblouisutdml-bin 2.8.0-3 amd64 Braille UTDML translation utilities
ii liblouisutdml-data 2.8.0-3 all Braille UTDML translation library - data
ii liblouisutdml9 2.8.0-3 amd64 Braille UTDML translation library - shared libs
ii liblsan0 10-20200411-0ubuntu1 amd64 LeakSanitizer -- a memory leak detector (runtime)
ii libltdl-dev 2.4.6-14 amd64 System independent dlopen wrapper for GNU libtool
ii libltdl7 2.4.6-14 amd64 System independent dlopen wrapper for GNU libtool

```

```

ii liblLua5.2-0 5.2.4-1.1build3 amd64 Shared library for the Lua interpreter version 5.2
ii liblLua5.3-0 5.3.3-1.1ubuntu2 amd64 Shared library for the Lua interpreter version 5.3
ii liblwp-mediatypes-perl 6.04-1 all module to guess media type for a file or a URL
ii liblwp-protocol-https-perl 6.07-2ubuntu2 all HTTPS driver for LWP::UserAgent
ii liblz4-1 1.9.2-2 amd64 Fast LZ compression algorithm library - runtime
ii liblzma5 5.2.4-1 amd64 XZ-format compression library
ii liblzoz2-2 2.10-2 amd64 data compression library
ii libmagic-mgc 1:5.38-4 amd64 File type determination library using "magic" numbers (compiled magic file)
ii libmagic1 1:5.38-4 amd64 Recognize the type of data in a file using "magic" numbers - library
ii libmail-sendmail-perl 0.80-1 all simple way to send email from a perl script
ii libmailtools-perl 2.21-1 all modules to manipulate email in perl programs
ii libmaxminddb0 1.4.2-0ubuntu1 amd64 IP geolocation database library
ii libmbim-glib4 1.22.0-2 amd64 Support library to use the MBIM protocol
ii libmbim-proxy 1.22.0-2 amd64 Proxy to communicate with MBIM ports
ii libmcrypt4 2.5.8-3.4 amd64 De-/Encryption Library
ii libmediaart-2.0-0 1.9.4-2 amd64 media art extraction and cache management library
ii libmessaging-menu0 13.10.1+18.10.20180918-0ubuntu2 amd64 Messaging Menu - shared library
ii libmhash2 0.9.9.9-8 amd64 Library for cryptographic hashing and message authentication
ii libminiuPnPc17 2.1.20190824-0ubuntu2 amd64 UPnP IGD client lightweight library
ii libmm-glib0 1.12.8-1 amd64 D-Bus service for managing modems - shared libraries
ii libmnml0 1.0.4-2 amd64 minimalistic Netlink communication library
ii libmount1 2.34-0.1ubuntu9 amd64 device mounting library
ii libmozjs-68-0 68.6.0-1ubuntu1 amd64 SpiderMonkey JavaScript library
ii libmp3lame0 3.100-3 amd64 MP3 encoding library
ii libmpc3 1.1.0-1 amd64 multiple precision complex floating-point library
ii libmpdec2 2.4.2-3 amd64 library for decimal floating point arithmetic (runtime library)
ii libmpfr6 4.0.2-1 amd64 multiple precision floating-point computation
ii libmpg123-0 1.25.13-1 amd64 MPEG layer 1/2/3 audio decoder (shared library)
ii libmspack0 0.10.1-2 amd64 library for Microsoft compression formats (shared library)
ii libmspub-0.1-1 0.1.4-1build3 amd64 library for parsing the mspub file structure
ii libmtdev1 1.1.5-1.1 amd64 Multitouch Protocol Translation Library - shared library
ii libmt-common 1.1.17-3 all Media Transfer Protocol (MTP) common files
ii libmt-runtime 1.1.17-3 amd64 Media Transfer Protocol (MTP) runtime tools
ii libmt9 1.1.17-3 amd64 Media Transfer Protocol (MTP) library
ii libmutter-6-0 3.36.3-0ubuntu0.20.04.1 amd64 window manager library from the Mutter window manager
ii libmwaw-0.3-3 0.3.15-2build1 amd64 import library for some old Mac text documents
ii libmysqclient21 8.0.21-0ubuntu0.20.04.3 amd64 MySQL database client library
ii libmythes-1.2-0 2:1.2.4-3build1 amd64 simple thesaurus library
ii libnatppm1 20150609-7build1 amd64 portable and fully compliant implementation of NAT-PMP
ii libnautilus-extension1a 1:3.36.3-0ubuntu1 amd64 libraries for nautilus components - runtime version
ii libncurses6 6.2-0ubuntu2 amd64 shared libraries for terminal handling
ii libncursesw6 6.2-0ubuntu2 amd64 shared libraries for terminal handling (wide character support)
ii libndp0 1.7-0ubuntu1 amd64 Library for Neighbor Discovery Protocol
ii libneon27-gnutls 0.30.2-4 amd64 HTTP and WebDAV client library (GnuTLS enabled)
ii libnet-dbus-perl 1.2.0-1 amd64 Perl extension for the DBus bindings
ii libnet-http-perl 6.19-1 all module providing low-level HTTP connection client
ii libnet-smtp-ssl-perl 1.04-1 all Perl module providing SSL support to Net::SMTP
ii libnet-ssleay-perl 1.88-2ubuntu1 amd64 Perl module for Secure Sockets Layer (SSL)
ii libnetfilter-contrack3 1.0.7-2 amd64 Netfilter netlink-contrack library
ii libnetplan0 0.99-0ubuntu3-20.04.2 amd64 YAML network configuration abstraction runtime library
ii libnettle7 3.5.1+really3.5.1-2 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52.21-4ubuntu2 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnetlink0 1.0.1-3build1 amd64 Netfilter netlink library
ii libnfs13 4.0.0-1 amd64 NFS client library (shared library)
ii libnftnl11 1.1.5-1 amd64 Netfilter nftables userspace API library
ii libnghttp2-14 1.40.0-1build1 amd64 library implementing HTTP/2 protocol (shared library)
ii libnl-3-200 3.4.0-1 amd64 library for dealing with netlink sockets
ii libnl-genl-3-200 3.4.0-1 amd64 library for dealing with netlink sockets - generic netlink
ii libnl-route-3-200 3.4.0-1 amd64 library for dealing with netlink sockets - route interface
ii libnm0 1.22.10-1ubuntu2.1 amd64 GObject-based client library for NetworkManager
ii libnm0 1.8.24-1ubuntu2 amd64 library for wireless and mobile dialogs (libnm version)
ii libnotify-bin 0.7.9-1ubuntu2 amd64 sends desktop notifications to a notification daemon (Utilities)
ii libnotify4 0.7.9-1ubuntu2 amd64 sends desktop notifications to a notification daemon
ii libnpth0 1.6-1 amd64 replacement for GNU Pth using system threads
ii libnsp4 2:4.25-1 amd64 NetScape Portable Runtime Library
ii libnss-mdns 0.14.1-1ubuntu1 amd64 NSS module for Multicast DNS name resolution
ii libnss-systemd 245.4-4ubuntu3.2 amd64 nss module providing dynamic user and group name resolution
ii libnss3 2:3.49.1-1ubuntu1.2 amd64 Network Security Service libraries
ii libntfs-3g883 1:2017.3.23AR.3-3ubuntu1 amd64 read/write NTFS driver for FUSE (runtime library)
ii libnuma1 2.0.12-1 amd64 Libraries for controlling NUMA policy
ii libodfgen-0.1-1 0.1.7-1ubuntu2 amd64 library to generate ODF documents
ii libogg0 1.3.4-0ubuntu1 amd64 Ogg bitstream library
ii libopenjp2-7 2.3.1-1ubuntu4 amd64 JPEG 2000 image compression/decompression library
ii libopus0 1.3.1-0ubuntu1 amd64 Opus codec runtime library
ii liborc-0.4-0 1:0.4.31-1 amd64 Library of Optimized Inner Loops Runtime Compiler
ii liborcus-0.15-0 0.15.3-3build2 amd64 library for processing spreadsheet documents
ii libp11-kit0 0.23.20-1build1 amd64 library for loading and coordinating access to PKCS#11 modules - runtime
ii libpackagekit-glib2-18 1.1.13-2ubuntu1 amd64 Library for accessing PackageKit using Glib
ii libpagemaker-0.0-0 0.0.4-1build1 amd64 Library for importing and converting PageMaker Documents
ii libpam-cap 1:2.32-1 amd64 POSIX 1003.1e capabilities (PAM module)
ii libpam-fprintd 1.90.1-1ubuntu1 amd64 PAM module for fingerprint authentication through fprintf
ii libpam-gnome-keyring 3.36.0-1ubuntu1 amd64 PAM module to unlock the GNOME keyring upon login
ii libpam-modules 1.3.1-Subuntu4 amd64 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.3.1-5ubuntu4 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.3.1-5ubuntu4 all Runtime support for the PAM library
ii libpam-systemd 245.4-4ubuntu3.2 amd64 system and service manager - PAM module
ii libpam0g 1.3.1-5ubuntu4 amd64 Pluggable Authentication Modules library
ii libpango-1.0-0 1.44.7-2ubuntu4 amd64 Layout and rendering of internationalized text
ii libpangocairo-1.0-0 1.44.7-2ubuntu4 amd64 Layout and rendering of internationalized text
ii libpangoft2-1.0-0 1.44.7-2ubuntu4 amd64 Layout and rendering of internationalized text
ii libpangomm-1.4-1v5 2.42.0-2build1 amd64 C++ Wrapper for pango (shared libraries)
ii libpangooxft-1.0-0 1.44.7-2ubuntu4 amd64 Layout and rendering of internationalized text
ii libpaper-utils 1.1.28 amd64 library for handling paper characteristics (utilities)
ii libpaper1 1.1.28 amd64 library for handling paper characteristics
ii libparted-fs-resize0 3.3-4 amd64 disk partition manipulator - shared FS resizing library
ii libparted2 3.3-4 amd64 disk partition manipulator - shared library
ii libpcap0.8 1.9.1-3 amd64 System interface for user-level packet capture
ii libpcaudio0 1.1-4 amd64 C API to different audio devices - shared library
ii libpci3 1:3.6.4-1 amd64 PCI utilities (shared library)

```

```

ii libpciaccess0 0.16-0ubuntu1 amd64 Generic PCI access library for X
ii libpcre16-3 2:8.44-1+ubuntu20.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - 16 bit runtime files
ii libpcre2-32-0 10.35-4+ubuntu20.04.1+deb.sury.org+1 amd64 New Perl Compatible Regular Expression Library - 32 bit runtime files
ii libpcre2-8-0 10.35-4+ubuntu20.04.1+deb.sury.org+1 amd64 New Perl Compatible Regular Expression Library- 8 bit runtime files
ii libpcre3 2:8.44-1+ubuntu20.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - runtime files
ii libpcre3-dev 2:8.44-1+ubuntu20.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - development files
ii libpcre32-3 2:8.44-1+ubuntu20.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - 32 bit runtime files
ii libpcrecpp0v5 2:8.44-1+ubuntu20.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - C++ runtime files
ii libpccslite1 1.8.26-3 amd64 Middleware to access a smart card using PC/SC (library)
ii libpeas-1.0-0 1.26.0-2 amd64 Application plugin library
ii libpeas-common 1.26.0-2 all Application plugin library (common files)
ii libperl5.30 5.30.0-9build1 amd64 shared Perl library
ii libphonenumber7 7.1.0-5ubuntu11 amd64 parsing/formatting/validating phone numbers
ii libpipeline1 1.5.2-2build1 amd64 Unix process pipeline manipulation library
ii libpixman-1-0 0.38.4-0ubuntu1 amd64 pixel-manipulation library for X and cairo
ii libpkcs11-helper1 2.16.1-1 amd64 library that simplifies the interaction with PKCS#11
ii libplist3 2.1.0-4build2 amd64 Library for handling Apple binary and XML property lists
ii libplymouth5 0.9.4git20200323-0ubuntu6 amd64 graphical boot animation and logger - shared libraries
ii libpng16-16 1.6.37-2 amd64 PNG library - runtime (version 1.6)
ii libpolkit-agent-1-0 0.105-26ubuntu1 amd64 PolicyKit Authentication Agent API
ii libpolkit-gobject-1-0 0.105-26ubuntu1 amd64 PolicyKit Authorization API
ii libpoppler-cpp0v5 0.86.1-0ubuntu1 amd64 PDF rendering library (CPP shared library)
ii libpoppler-glib8 0.86.1-0ubuntu1 amd64 PDF rendering library (GLib-based shared library)
ii libpoppler97 0.86.1-0ubuntu1 amd64 PDF rendering library
ii libpopt0 1.16-14 amd64 lib for parsing cmdline parameters
ii libprocps8 2:3.3.16-1ubuntu2 amd64 library for accessing process information from /proc
ii libprotobuf17 3.6.1.3-2ubuntu5 amd64 protocol buffers C++ library
ii libproxy1-plugin-gsettings 0.4.15-10ubuntu1 amd64 automatic proxy configuration management library (GSettings plugin)
ii libproxy1-plugin-networkmanager 0.4.15-10ubuntu1 amd64 automatic proxy configuration management library (Network Manager plugin)
ii libproxy1v5 0.4.15-10ubuntu1 amd64 automatic proxy configuration management library (shared)
ii libpsl5 0.21.0-1ubuntu1 amd64 Library for Public Suffix List (shared libraries)
ii libpulse-mainloop-glib0 1:13.99.1-1ubuntu3.5 amd64 PulseAudio client libraries (glib support)
ii libpulse0 1:13.99.1-1ubuntu3.5 amd64 PulseAudio client libraries
ii libpulsedsp 1:13.99.1-1ubuntu3.5 amd64 PulseAudio OSS pre-load library
ii libpwquality-common 1.4.2-1build1 all library for password quality checking and generation (data files)
ii libpwquality1 1.4.2-1build1 amd64 library for password quality checking and generation
ii libpython3-stdlib 3.8.2-0ubuntu2 amd64 interactive high-level object-oriented language (default python3 version)
ii libpython3.8 3.8.2-1ubuntu1.2 amd64 Shared Python runtime library (version 3.8)
ii libpython3.8-minimal 3.8.2-1ubuntu1.2 amd64 Minimal subset of the Python language (version 3.8)
ii libpython3.8-stdlib 3.8.2-1ubuntu1.2 amd64 Interactive high-level object-oriented language (standard library, version 3.8)
ii libqmi-glib5 1.24.8-1 amd64 Support library to use the Qualcomm MSM Interface (QMI) protocol
ii libqmi-proxy 1.24.8-1 amd64 Proxy to communicate with QMI ports
ii libqpdf26 9.1.1-1build1 amd64 runtime library for PDF transformation/inspection software
ii libqqwing2v5 1.3.4-1.1build1 amd64 tool for generating and solving Sudoku puzzles (library)
ii libquadmath0 10-20200411-0ubuntu1 amd64 GCC Quad-Precision Math Library
ii librados2 15.2.3-0ubuntu0.20.04.1 amd64 RADOS distributed object store client library
ii libraptor2-0 2.0.15-0ubuntu1 amd64 Raptor 2 RDF syntax library
ii librasql3 0.9.33-0.1 amd64 Rasql RDF query library
ii libraw1394-11 2.1.2-1 amd64 library for direct access to IEEE 1394 bus (aka FireWire)
ii libraw19 0.19.5-1ubuntu1 amd64 raw image decoder library
ii librdfl0 1.0.17-1.1ubuntu1 amd64 Redland Resource Description Framework (RDF) library
ii librdmacm1 28.0-1ubuntu1 amd64 Library for managing RDMA connections
ii libreadline5 5.2+dfsg-3build3 amd64 GNU readline and history libraries, run-time libraries
ii libreadline8 8.0-4 amd64 GNU readline and history libraries, run-time libraries
ii libreoffice-base-core 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- shared library
ii libreoffice-calc 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- spreadsheet
ii libreoffice-common 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- arch-independent files
ii libreoffice-core 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- arch-dependent files
ii libreoffice-draw 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- drawing
ii libreoffice-gnome 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- GNOME integration
ii libreoffice-gtk3 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- GTK+ 3 integration
ii libreoffice-help-common 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- common files for LibreOffice help
ii libreoffice-help-de 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- German help
ii libreoffice-help-en-gb 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- English_british help
ii libreoffice-help-en-us 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- English_american help
ii libreoffice-impress 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- presentation
ii libreoffice-l10n-de 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- German language package
ii libreoffice-l10n-en-gb 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- English_british language package
ii libreoffice-l10n-en-za 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- English_southafrican language package
ii libreoffice-math 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- equation editor
ii libreoffice-ogltrans 1:6.4.4-0ubuntu0.20.04.1 all transitional package for libreoffice-ogltrans
ii libreoffice-pdfimport 1:6.4.4-0ubuntu0.20.04.1 all transitional package for PDF Import component for LibreOffice
ii libreoffice-style-breeze 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- Breeze symbol style
ii libreoffice-style-colibre 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- colibre symbol style
ii libreoffice-style-elementary 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- Elementary symbol style
ii libreoffice-style-tango 1:6.4.4-0ubuntu0.20.04.1 all office productivity suite -- Tango symbol style
ii libreoffice-writer 1:6.4.4-0ubuntu0.20.04.1 amd64 office productivity suite -- word processor
ii librest-0.7-0 0.8.1-1 amd64 REST service access library
ii libreveng-0.0-0 0.0.4-6ubuntu5 amd64 Base Library for writing document interface filters
ii librhythmbox-core10 3.4.4-1ubuntu2 amd64 support library for the rhythmbox music player
ii libridl-javaplugin 1:6.4.4-0ubuntu0.20.04.1 all LibreOffice UNO runtime environment -- base types and types access library for the Java Uno typesystem
ii libroken18-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - roken support library
ii librsvg2-2 2.48.7-1ubuntu0.20.04.1 amd64 SAX-based renderer library for SVG files (runtime)
ii librsvg2-common 2.48.7-1ubuntu0.20.04.1 amd64 SAX-based renderer library for SVG files (extra runtime)
ii librsvg2c 2.0.2-1ubuntu1 amd64 rsync remote-delta algorithm library
ii librtmp1 2.4+20151223.gitfa8646d.1-2build1 amd64 toolkit for RTMP streams (shared library)
ii librygel-core-2.6-2 0.38.3-1ubuntu1 amd64 GNOME UPnP/DLNA services - core library
ii librygel-db-2.6-2 0.38.3-1ubuntu1 amd64 GNOME UPnP/DLNA services - db library
ii librygel-renderer-2.6-2 0.38.3-1ubuntu1 amd64 GNOME UPnP/DLNA services - renderer library
ii librygel-server-2.6-2 0.38.3-1ubuntu1 amd64 GNOME UPnP/DLNA services - server library
ii libsamplerate0 0.1.9-2 amd64 Audio sample rate conversion library
ii lib sane 1.0.29-0ubuntu5 amd64 API library for scanners
ii lib sane-common 1.0.29-0ubuntu5 all API library for scanners -- documentation and support files
ii lib sane-hpaio 3.20.3+dfsg0-2 amd64 HP SANE backend for multi-function peripherals
ii lib sasl2-2 2.1.27+dfsg-2 amd64 Cyrus SASL - authentication abstraction library
ii lib sasl2-modules 2.1.27+dfsg-2 amd64 Cyrus SASL - pluggable authentication modules
ii lib sasl2-modules-db 2.1.27+dfsg-2 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii lib sbsc1 1.4-1 amd64 Sub Band CODEC library - runtime

```

```

ii libseccomp2 2.4.3-1ubuntu3.20.04.3 amd64 high level interface to Linux seccomp filter
ii libsecret-1-0 0.20.3-0ubuntu1 amd64 Secret store
ii libsecret-common 0.20.3-0ubuntu1 all Secret store (common files)
ii libselinux1 3.0-1build2 amd64 SELinux runtime shared libraries
ii libsemanage-common 3.0-1build2 all Common files for SELinux policy management libraries
ii libsemanage1 3.0-1build2 amd64 SELinux policy management library
ii libsensors-config 1:3.6.0-2ubuntu1 all lm-sensors configuration files
ii libsensors5 1:3.6.0-2ubuntu1 amd64 library to read temperature/voltage/fan sensors
ii libsepolicy 3.0-1 amd64 SELinux library for manipulating binary security policies
ii libsgutils2-2 1.44-1ubuntu2 amd64 utilities for devices using the SCSI command set (shared libraries)
ii libshout3 2.4.3-1 amd64 MP3/Ogg Vorbis broadcast streaming library
ii libsigc++-2.0-0v5 2.10.2-1build1 amd64 type-safe Signal Framework for C++ - runtime
ii libsigsegv2 2.12-2 amd64 Library for handling page faults in a portable way
ii libsslang2 2.3.2-4 amd64 S-Lang programming library - runtime version
ii libsm6 2:1.2.3-1 amd64 X11 Session Management library
ii libsmartcols1 2.34-0.1ubuntu9 amd64 smart column output alignment library
ii lib smbclient 2:4.11.6+dfsg-0ubuntu1.3 amd64 shared library for communication with SMB/CIFS servers
ii lib smbios-c2 2.4.3-1 amd64 Provide access to (SM)BIOS information -- dynamic library
ii libsnappy 1.57-0ubuntu3 amd64 GLib snapd library
ii libsnappy1v5 1.1.8-1build1 amd64 fast compression/decompression library
ii libsndfile1 1.0.28-7 amd64 Library for reading/writing audio files
ii libsnmp-base 5.8+dfsg-2ubuntu2.2 all SNMP configuration script, MIBs and documentation
ii libsnmp35 5.8+dfsg-2ubuntu2.2 amd64 SNMP (Simple Network Management Protocol) library
ii libodium23 1.0.18-1 amd64 Network communication, cryptography and signaturing library
ii libsonic0 0.2.0-8 amd64 Simple library to speed up or slow down speech
ii libsoup-gnome2.4-1 2.70.0-1 amd64 HTTP library implementation in C -- GNOME support library
ii libsoup2.4-1 2.70.0-1 amd64 HTTP library implementation in C -- Shared library
ii libsoxr0 0.1.3-2build1 amd64 High quality 1D sample-rate conversion library
ii libspectre1 0.2.8-2 amd64 Library for rendering PostScript documents
ii libspeexhd2 0.9.1-4 amd64 Speech Dispatcher: Shared libraries
ii libspeex1 1.2~rc1.2-1.1ubuntu1 amd64 The Speex codec runtime library
ii libspeexdsp1 1.2~rc1.2-1.1ubuntu1 amd64 The Speex extended runtime library
ii libsqlite3-0 3.31.1-4ubuntu0.2 amd64 SQLite 3 shared library
ii libss2 1.45.5-2ubuntu1 amd64 command-line interface parsing library
ii libssh-4 0.9.3-2ubuntu2 amd64 tiny C SSH library (OpenSSL flavor)
ii libssl-dev 1.1.1g-1ubuntu20.04.1+deb.sury.org+1 amd64 Secure Sockets Layer toolkit - development files
ii libssl1.1 1.1.1g-1ubuntu20.04.1+deb.sury.org+1 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstartupper-notification0 0.12-6 amd64 library for program launch feedback (shared library)
ii libstdc++-9-dev 9.3.0-10ubuntu2 amd64 GNU Standard C++ Library v3 (development files)
ii libstdc++6 10-20200411-0ubuntu1 amd64 GNU Standard C++ Library v3
ii libstemmer0d 0+svn585-2 amd64 Snowball stemming algorithms for use in Information Retrieval
ii libsub-override-perl 0.09-2 all Perl module used to temporarily override subroutines
ii libsuitesparseconfig5 1:5.7.1+dfsg-2 amd64 configuration routines for all SuiteSparse modules
ii libsynctex2 2019.20190605.51237-3build2 amd64 TeX Live: SyncTeX parser library
ii libsys-hostname-long-perl 1.5-1 all Figure out the long (fully-qualified) hostname
ii libsysmetrics1 1.6.1 amd64 Report hardware and other collected metrics - shared lib
ii libsystemd0 245.4-4ubuntu3.2 amd64 systemd utility library
ii libtag1v5 1.11.1+dfsg.1-0.3ubuntu2 amd64 audio meta-data library
ii libtag1v5-vanilla 1.11.1+dfsg.1-0.3ubuntu2 amd64 audio meta-data library - vanilla flavour
ii libtalloc2 2.3.0-3ubuntu1 amd64 hierarchical pool based memory allocator
ii libtasn1-6 4.16.0-2 amd64 Manage ASN.1 structures (runtime)
ii libtdb1 1.4.2-3build1 amd64 Trivial Database - shared library
ii libteamdctl0 1.30-1 amd64 library for communication with `teamd` process
ii libtepl-4-0 4.4.0-1 amd64 Text editor library for GTK
ii libterm-readkey-perl 2.38-1build1 amd64 perl module for simple terminal control
ii libtevent0 0.10.1-4 amd64 talloc-based event loop library - shared library
ii libtext-charwidth-perl 0.04-10 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-7 amd64 module to convert between character sets in Perl
ii libtext-wrapi8n-perl 0.06-9 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.28-3 all Data files for Thai language support library
ii libthai0 0.1.28-3 amd64 Thai language support library
ii libtheora0 1.1.1+dfsg.1-15ubuntu2 amd64 Theora Video Compression Codec
ii libtie-ixhash-perl 1.23-2 all Perl module to order associative arrays
ii libtiff5 4.1.0+git191117-2build1 amd64 Tag Image File Format (TIFF) library
ii libtimedate-perl 2.3200-1 all collection of modules to manipulate date/time information
ii libtinfo6 6.2-0ubuntu2 amd64 shared low-level terminfo library for terminal handling
ii libtool 2.4.6-14 all Generic library support script
ii libtotem-plparser-common 3.26.5-1ubuntu1 all Totem Playlist Parser library - common files
ii libtotem-plparser18 3.26.5-1ubuntu1 amd64 Totem Playlist Parser library - runtime files
ii libtotem0 3.34.1-2ubuntu2 amd64 Main library for the Totem media player
ii libtracker-control-2.0-0 2.3.4-1 amd64 library to control/monitor tracker miners
ii libtracker-miner-2.0-0 2.3.4-1 amd64 tracker data miner library
ii libtracker-sparql2-0.0-0 2.3.4-1 amd64 metadata database, indexer and search tool - library
ii libtry-tiny-perl 0.30-1 all module providing minimalistic try/catch
ii libtsan0 10-20200411-0ubuntu1 amd64 ThreadSanitizer -- a Valgrind-based detector of data races (runtime)
ii libtss2-esys0 2.3.2-1 amd64 TPM2 Software stack library - TSS and TCTI libraries
ii libtwolame0 0.4.0-2 amd64 MPEG Audio Layer 2 encoding library
ii libu2f-udev 1.1.10-1 all Universal 2nd Factor (U2F) common files
ii libubsan1 10-20200411-0ubuntu1 amd64 UBSan -- undefined behaviour sanitizer (runtime)
ii libuchardet0 0.0.6-3build1 amd64 universal charset detection library - shared library
ii libudev1 245.4-4ubuntu3.2 amd64 libudev shared library
ii libudisks2-0 2.8.4-1ubuntu1 amd64 GObject based library to access udisks2
ii libunistring2 0.9.10-2 amd64 Unicode string library for C
ii libunity-protocol-private7 7.1.4+19.04.20190319-0ubuntu3 amd64 binding to get places into the launcher - private library
ii libunity-scopes-json-def-desktop 7.1.4+19.04.20190319-0ubuntu3 all binding to get places into the launcher - desktop def file
ii libunity9 7.1.4+19.04.20190319-0ubuntu3 amd64 binding to get places into the launcher - shared library
ii libuno-cppu3 1:6.4.4-0ubuntu0.20.04.1 amd64 LibreOffice UNO runtime environment -- CPPU public library
ii libuno-cppuhelpergcc3-3 1:6.4.4-0ubuntu0.20.04.1 amd64 LibreOffice UNO runtime environment -- CPPU helper library
ii libuno-purpervhelpergcc3-3 1:6.4.4-0ubuntu0.20.04.1 amd64 LibreOffice UNO runtime environment -- "purpose environment" helper
ii libuno-sal3 1:6.4.4-0ubuntu0.20.04.1 amd64 LibreOffice UNO runtime environment -- SAL public library
ii libuno-salhelpergcc3-3 1:6.4.4-0ubuntu0.20.04.1 amd64 LibreOffice UNO runtime environment -- SAL helpers for C++ library
ii libunoloader-java 1:6.4.4-0ubuntu0.20.04.1 all LibreOffice UNO runtime environment -- (Java) UNO loader
ii libunwind8 1.2.1-9build1 amd64 library to determine the call-chain of a program - runtime
ii libupower-glib3 0.99.11-1build2 amd64 abstraction for power management - shared library
ii liburi-perl 1.76-2 all module to manipulate and access URI strings
ii libusb-1.0-0 2:1.0.23-2build1 amd64 userspace USB programming library
ii libusbxmud6 2.0.1-2 amd64 USB multiplexor daemon for iPhone and iPod Touch devices - library
ii libuuid1 2.34-0.1ubuntu9 amd64 Universally Unique ID library
ii libuv1 1.34.2-1ubuntu1 amd64 asynchronous event notification library - runtime library

```

```

ii libv4l-0 1.18.0-2build1 amd64 Collection of video4linux support libraries
ii libv4lconvert0 1.18.0-2build1 amd64 Video4linux frame format conversion library
ii libvisio-0.1-1 0.1.7-1build2 amd64 library for parsing the visio file structure
ii libvisual-0.4-0 0.4.0-17 amd64 audio visualization framework
ii libvncclient0 0.9.12+dfsg-9ubuntu0.2 amd64 API to write one's own VNC server - client library
ii libvolume-key1 0.3.12-3.1 amd64 Library for manipulating storage encryption keys and passphrases
ii libvorbis0a 1.3.6-2ubuntu1 amd64 decoder library for Vorbis General Audio Compression Codec
ii libvorbisenc2 1.3.6-2ubuntu1 amd64 encoder library for Vorbis General Audio Compression Codec
ii libvorbisfile3 1.3.6-2ubuntu1 amd64 high-level API for Vorbis General Audio Compression Codec
ii libvpnx6 1.8.2-1build1 amd64 VP8 and VP9 video codec (shared library)
ii libvte-2.91-0 0.60.3-0ubuntu1~20.04 amd64 Terminal emulator widget for GTK+ 3.0 - runtime files
ii libvte-2.91-common 0.60.3-0ubuntu1~20.04 amd64 Terminal emulator widget for GTK+ 3.0 - common files
ii libvulkan1 1.2.131.2-1 amd64 Vulkan loader library
ii libwacom-bin 1.3-2ubuntu1 amd64 Wacom model feature query library -- binaries
ii libwacom-common 1.3-2ubuntu1 all Wacom model feature query library (common files)
ii libwacom2 1.3-2ubuntu1 amd64 Wacom model feature query library
ii libwavpack1 5.2.0-1 amd64 audio codec (lossy and lossless) - library
ii libwayland-client0 1.18.0-1 amd64 wayland compositor infrastructure - client library
ii libwayland-cursor0 1.18.0-1 amd64 wayland compositor infrastructure - cursor library
ii libwayland-egl1 1.18.0-1 amd64 wayland compositor infrastructure - EGL library
ii libwayland-server0 1.18.0-1 amd64 wayland compositor infrastructure - server library
ii libwbclient0 2:4.11.6+dfsg-0ubuntu1.3 amd64 Samba winbind client library
ii libwebkit2gtk-4.0-37 2.28.3-0ubuntu0.20.04.1 amd64 Web content engine library for GTK
ii libwebp6 0.6.1-2 amd64 Lossy compression of digital photographic images.
ii libwebpdemux2 0.6.1-2 amd64 Lossy compression of digital photographic images.
ii libwebpmux3 0.6.1-2 amd64 Lossy compression of digital photographic images.
ii libwebrtc-audio-processing1 0.3.1-0ubuntu3 amd64 AudioProcessing module from the WebRTC project.
ii libwhoopsie-preferences0 22 amd64 Ubuntu error tracker submission settings - shared library
ii libwhoopsie0 0.2.69 amd64 Ubuntu error tracker submission - shared library
ii libwind0-heimdal 7.7.0+dfsg-1ubuntu1 amd64 Heimdal Kerberos - stringprep implementation
ii libwinpr2-2 2.1.1+dfsg1-0ubuntu0.20.04.1 amd64 Windows Portable Runtime library
ii libwmf0.2-7 0.2.8.4-17ubuntu1 amd64 Windows metafile conversion library
ii libwmf0.2-7-gtk 0.2.8.4-17ubuntu1 amd64 Windows metafile conversion library
ii libwnck-3-0 3.36.0-1 amd64 Window Navigator Construction Kit - runtime files
ii libwnck-3-common 3.36.0-1 all Window Navigator Construction Kit - common files
ii libwoff1 1.0.2-1build2 amd64 library for converting fonts to WOFF 2.0
ii libwpd-0.10-10 0.10.3-1build1 amd64 Library for handling WordPerfect documents (shared library)
ii libwpng-0.3-3 0.3.3-1build1 amd64 WordPerfect graphics import/convert library (shared library)
ii libwps-0.4-4 0.4.10-1build1 amd64 Works text file format import filter library (shared library)
ii libwrap0 7.6.q-30 amd64 Wietse Venema's TCP wrappers library
ii libwww-perl 6.43-1 all simple and consistent interface to the world-wide web
ii libwww-robotrules-perl 6.02-1 all database of robots.txt-derived permissions
ii libx11-6 2:1.6.9-2ubuntu1 amd64 X11 client-side library
ii libx11-data 2:1.6.9-2ubuntu1 all X11 client-side library
ii libx11-protocol-perl 0.56-7 all Perl module for the X Window System Protocol, version 11
ii libx11-xcb1 2:1.6.9-2ubuntu1 amd64 Xlib/XCB interface library
ii libxatracker2 20.0.8-0ubuntu1~20.04.1 amd64 X acceleration library -- runtime
ii libxaug1 1:1.0.9-0ubuntu1 amd64 X11 authorisation library
ii libxaw7 2:1.0.13-1 amd64 X11 Athena Widget library
ii libxcb-dri2-0 1.14-2 amd64 X C Binding, dri2 extension
ii libxcb-dri3-0 1.14-2 amd64 X C Binding, dri3 extension
ii libxcb-glx0 1.14-2 amd64 X C Binding, glx extension
ii libxcb-icccm4 0.4.1-1.1 amd64 utility libraries for X C Binding -- icccm
ii libxcb-image0 0.4.0-1build1 amd64 utility libraries for X C Binding -- image
ii libxcb-keysyms1 0.4.0-1build1 amd64 utility libraries for X C Binding -- keysyms
ii libxcb-present0 1.14-2 amd64 X C Binding, present extension
ii libxcb-randr0 1.14-2 amd64 X C Binding, randr extension
ii libxcb-render-util0 0.3.9-1build1 amd64 utility libraries for X C Binding -- render-util
ii libxcb-render0 1.14-2 amd64 X C Binding, render extension
ii libxcb-res0 1.14-2 amd64 X C Binding, res extension
ii libxcb-shape0 1.14-2 amd64 X C Binding, shape extension
ii libxcb-shm0 1.14-2 amd64 X C Binding, shm extension
ii libxcb-sync1 1.14-2 amd64 X C Binding, sync extension
ii libxcb-util1 0.4.0-0ubuntu3 amd64 utility libraries for X C Binding -- atom, aux and event
ii libxcb-xfixes0 1.14-2 amd64 X C Binding, xfixes extension
ii libxcb-xkb1 1.14-2 amd64 X C Binding, XKEYBOARD extension
ii libxcb-xv0 1.14-2 amd64 X C Binding, xv extension
ii libxcb1 1.14-2 amd64 X C Binding
ii libcomposite1 1:0.4.5-1 amd64 X11 Composite extension library
ii libxcursor1 1:1.2.0-2 amd64 X cursor management library
ii libxdamage1 1:1.1.5-2 amd64 X11 damaged region extension library
ii libxdmcp6 1:1.1.3-0ubuntu1 amd64 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.4-0ubuntu1 amd64 X11 miscellaneous extension library
ii libxfixed3 1:5.0.3-2 amd64 X11 miscellaneous 'fixes' extension library
ii libxfont2 1:2.0.3-1 amd64 X11 font rasterisation library
ii libxft2 2.3.3-0ubuntu1 amd64 FreeType-based font drawing library for X
ii libxi6 2:1.7.10-0ubuntu1 amd64 X11 Input extension library
ii libxinerama1 2:1.1.4-2 amd64 X11 Xinerama extension library
ii libxkbcommon-x11-0 0.10.0-1 amd64 library to create keymaps with the XKB X11 protocol
ii libxkbcommon0 0.10.0-1 amd64 library interface to the XKB compiler - shared library
ii libxkbfile1 1:1.1.0-1 amd64 X11 keyboard file manipulation library
ii libxklavier16 5.4-4 amd64 X Keyboard Extension high-level API
ii libxml-parser-perl 2.46-1 amd64 Perl module for parsing XML files
ii libxml-twig-perl 1:3.50-2 all Perl module for processing huge XML documents in tree mode
ii libxml-xpathengine-perl 0.14-1 all re-usable XPath engine for DOM-like trees
ii libxml2 2.9.10+dfsg-5+ubuntu20.04.1+deb.sury.org+3 amd64 GNOME XML library
ii libxmlmb1 0.1.15-2 amd64 Binary XML library
ii libxmlrpc-epi0 0.54.2-1.2 amd64 XML-RPC request serialisation/deserialisation library
ii libxmlsec1 1.2.28-2 amd64 XML security library
ii libxmlsec1-nss 1.2.28-2 amd64 NSS engine for the XML security library
ii libxmlsec1-openssl 1.2.28-2 amd64 OpenSSL engine for the XML security library
ii libxmug6 2:1.1.3-0ubuntu1 amd64 X11 miscellaneous utility library
ii libxmlmu1 2:1.1.3-0ubuntu1 amd64 X11 miscellaneous micro-utility library
ii libxpmp4 1:3.5.12-1 amd64 X11 pixmap library
ii libxrandr2 2:1.5.2-0ubuntu1 amd64 XRandR extension library
ii libxrender1 1:0.9.10-1 amd64 X Rendering Extension client library
ii libxres1 2:1.2.0-4 amd64 X11 Resource extension library
ii libxshmfence1 1.3-1 amd64 X shared memory fences - shared library
ii libxslt1.1 1.1.34-4 amd64 XSLT 1.0 processing library - runtime library

```

```

ii libxss1 1:1.2.3-1 amd64 X11 Screen Saver extension library
ii libxt6 1:1.1.5-1 amd64 X11 toolkit intrinsics library
ii libxtables12 1.8.4-3ubuntu2 amd64 netfilter xtables library
ii libxtst6 2:1.2.3-1 amd64 X11 Testing -- Record extension library
ii libxv1 2:1.0.11-1 amd64 X11 Video extension library
ii libxvmc1 2:1.0.12-2 amd64 X11 Video extension library
ii libxxf86dga1 2:1.1.5-0ubuntu1 amd64 X11 Direct Graphics Access extension library
ii libxxf86vm1 1:1.1.4-1build1 amd64 X11 XFree86 video mode extension library
ii libyajl2 2.1.0-3 amd64 Yet Another JSON Library
ii libyaml-0-2 0.2.2-1 amd64 Fast YAML 1.1 parser and emitter library
ii libyelp0 3.36.0-1 amd64 Library for the GNOME help browser
ii libzip4 1.6.1-3+ubuntu20.04.04+deb.sury.org+2 amd64 library for reading, creating, and modifying zip archives (runtime)
ii libzstd1 1.4.4+dfsg-3 amd64 fast lossless compression algorithm
ii linux-base 4.5ubuntu3.1 all Linux image base package
ii linux-firmware 1.187 all Firmware for Linux kernel drivers
ii linux-generic-hwe-20.04 5.4.0.42.45 amd64 Complete Generic Linux kernel and headers
ii linux-headers-5.4.0-26 5.4.0-26.30 all Header files related to Linux kernel version 5.4.0
ii linux-headers-5.4.0-26-generic 5.4.0-26.30 amd64 Linux kernel headers for version 5.4.0 on 64 bit x86 SMP
ii linux-headers-5.4.0-42 5.4.0-42.46 all Header files related to Linux kernel version 5.4.0
ii linux-headers-5.4.0-42-generic 5.4.0-42.46 amd64 Linux kernel headers for version 5.4.0 on 64 bit x86 SMP
ii linux-headers-generic-hwe-20.04 5.4.0.42.45 amd64 Generic Linux kernel headers
ii linux-image-5.4.0-26-generic 5.4.0-26.30 amd64 Signed kernel image generic
ii linux-image-5.4.0-42-generic 5.4.0-42.46 amd64 Signed kernel image generic
ii linux-image-generic-hwe-20.04 5.4.0.42.45 amd64 Generic Linux kernel image
ii linux-libc-dev 5.4.0-42.46 amd64 Linux Kernel Headers for development
ii linux-modules-5.4.0-26-generic 5.4.0-26.30 amd64 Linux kernel extra modules for version 5.4.0 on 64 bit x86 SMP
ii linux-modules-5.4.0-42-generic 5.4.0-42.46 amd64 Linux kernel extra modules for version 5.4.0 on 64 bit x86 SMP
ii linux-modules-extra-5.4.0-26-generic 5.4.0-26.30 amd64 Linux kernel extra modules for version 5.4.0 on 64 bit x86 SMP
ii linux-modules-extra-5.4.0-42-generic 5.4.0-42.46 amd64 Linux kernel extra modules for version 5.4.0 on 64 bit x86 SMP
ii linux-sound-base 1.0.25+dfsg-0ubuntu5 all base package for ALSA and OSS sound systems
ii locales 2.31-0ubuntu9 all GNU C Library: National Language (locale) data [support]
ii login 1:4.8.1-1ubuntu5.20.04 amd64 system login tools
ii logrotate 3.14.0-4ubuntu3 amd64 Log rotation utility
ii logsave 1.45.5-2ubuntu1 amd64 save the output of a command in a log file
ii lp-solve 5.5.0.15-4build1 amd64 Solve (mixed integer) linear programming problems
ii lsb-base 11.1.0ubuntu2 all Linux Standard Base init script functionality
ii lsb-release 11.1.0ubuntu2 all Linux Standard Base version reporting utility
ii lshw 02.18.85-0.3ubuntu2 amd64 information about hardware configuration
ii lsof 4.93.2+dfsg-1 amd64 utility to list open files
ii ltrace 0.7.3-6.1ubuntu1 amd64 Tracks runtime library calls in dynamically linked programs
ii lz4 1.9.2-2 amd64 Fast LZ compression algorithm - tool
ii m4 1.4.18-4 amd64 macro processing language
ii make 4.2.1.1-2 amd64 utility for directing compilation
ii man-db 2.9.1-1 amd64 tools for reading manual pages
ii manpages 5.05-1 all Manual pages about using a GNU/Linux system
ii manpages-dev 5.05-1 all Manual pages about using GNU/Linux for development
ii mariadb-client 1:10.3.22-1ubuntu1 all MariaDB database client (metapackage depending on the latest version)
ii mariadb-client-10.3 1:10.3.22-1ubuntu1 amd64 MariaDB database client binaries
ii mariadb-client-core-10.3 1:10.3.22-1ubuntu1 amd64 MariaDB database core client binaries
ii mariadb-common 1:10.3.22-1ubuntu1 all MariaDB common metapackage
ii mariadb-server 1:10.3.22-1ubuntu1 all MariaDB database server (metapackage depending on the latest version)
ii mariadb-server-10.3 1:10.3.22-1ubuntu1 amd64 MariaDB database server binaries
ii mariadb-server-core-10.3 1:10.3.22-1ubuntu1 amd64 MariaDB database core server files
ii mawk 1.3.4.20200120-2 amd64 Pattern scanning and text processing language
ii media-player-info 24-2 all Media player identification files
ii memtest86+ 5.01-3.1ubuntu1 amd64 thorough real-mode memory tester
ii mesa-vulkan-drivers 20.0.8-0ubuntu1~20.04.1 amd64 Mesa Vulkan graphics drivers
ii mime-support 3.64ubuntu1 all MIME files 'mime.types' & 'mailcap', and support programs
ii mobile-broadband-provider-info 20190618-3 all database of mobile broadband service providers
ii modemmanager 1.12.8-1 amd64 D-Bus service for managing modems
ii mount 2.34-0.1ubuntu9 amd64 tools for mounting and manipulating filesystems
ii mousetweaks 3.32.0-2 amd64 mouse accessibility enhancements for the GNOME desktop
ii mscompress 0.4-7 amd64 Microsoft "compress.exe/expand.exe" compatible (de)compressor
ii mtools 4.0.24-1 amd64 Tools for manipulating MSDOS files
ii mtr-tiny 0.93-1 amd64 Full screen ncurses traceroute tool
ii mutter 3.36.3-0ubuntu0.20.04.1 amd64 Example window manager using GNOME's window manager library
ii mutter-common 3.36.3-0ubuntu0.20.04.1 all shared files for the Mutter window manager
ii mysql-common 5.8+1.0.5ubuntu2 all MySQL database common files, e.g. /etc/mysql/my.cnf
ii mythes-de 20160424-3 all German Thesaurus for OpenOffice.org/LibreOffice
ii mythes-de-ch 20160424-3 all German Thesaurus for OpenOffice.org/LibreOffice (Swiss Version)
ii mythes-en-au 2.1-5.4 all Australian English Thesaurus for OpenOffice.org
ii mythes-en-us 1:6.4.3-1 all English (USA) Thesaurus for LibreOffice
ii nano 4.8-1ubuntu1 amd64 small, friendly text editor inspired by Pico
ii nautilus 1:3.36.3-0ubuntu1 amd64 file manager and graphical shell for GNOME
ii nautilus-data 1:3.36.3-0ubuntu1 all data files for nautilus
ii nautilus-extension-gnome-terminal 3.36.2-1ubuntu1~20.04 amd64 GNOME terminal emulator application - Nautilus extension
ii nautilus-sendto 3.8.6-3 amd64 easily send files via email from within Nautilus
ii nautilus-share 0.7.3-2ubuntu3 amd64 Nautilus extension to share folder using Samba
ii ncurses-base 6.2-0ubuntu2 all basic terminal type definitions
ii ncurses-bin 6.2-0ubuntu2 amd64 terminal-related programs and man pages
ii ncurses-term 6.2-0ubuntu2 all additional terminal type definitions
ii net-tools 1.60+git20180626.aebd88e-1ubuntu1 amd64 NET-3 networking toolkit
ii netbase 6.1 all Basic TCP/IP networking system
ii netcat-openbsd 1.206-1ubuntu1 amd64 TCP/IP swiss army knife
ii netplan.io 0.99-0ubuntu3~20.04.2 amd64 YAML network configuration abstraction for various backends
ii network-manager 1.22.10-1ubuntu2.1 amd64 network management framework (daemon and userspace tools)
ii network-manager-config-connectivity-ubuntu 1.22.10-1ubuntu2.1 all NetworkManager configuration to enable connectivity checking
ii network-manager-gnome 1.8.24-1ubuntu2 amd64 network management framework (GNOME frontend)
ii network-manager-openvpn 1.8.12-1 amd64 network management framework (OpenVPN plugin core)
ii network-manager-openvpn-gnome 1.8.12-1 amd64 network management framework (OpenVPN plugin GNOME GUI)
ii network-manager-pptp 1.2.8-2 amd64 network management framework (PPTP plugin core)
ii network-manager-pptp-gnome 1.2.8-2 amd64 network management framework (PPTP plugin GNOME GUI)
ii networkd-dispatcher 2.0.1-1 all Dispatcher service for systemd-networkd connection status changes
ii ntfs-3g 1:2017.3.23AR.3-3ubuntu1 amd64 read/write NTFS driver for FUSE
ii open-vm-tools 2:11.1.0-2~ubuntu20.04.1 amd64 Open VMware Tools for virtual machines hosted on VMware (CLI)
ii open-vm-tools-desktop 2:11.1.0-2~ubuntu20.04.1 amd64 Open VMware Tools for virtual machines hosted on VMware (GUI)
ii openprinting-ppds 20200401-1 all OpenPrinting printer support - PostScript PPD files
ii openssh-client 1:8.2p1-4ubuntu0.1 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:8.2p1-4ubuntu0.1 amd64 secure shell (SSH) server, for secure access from remote machines

```

```

ii openssh-sftp-server 1:8.2p1-4ubuntu0.1 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines
ii openssl 1.1.1g-1+ubuntu20.04.1+deb.sury.org+1 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii openvpn 2.4.7-1ubuntu2 amd64 virtual private network daemon
ii orca 3.36.2-1ubuntu1~20.04.1 all Scriptable screen reader
ii os-prober 1.74ubuntu2 amd64 utility to detect other OSes on a set of drives
ii p11-kit 0.23.20-1build1 amd64 p11-glue utilities
ii p11-kit-modules 0.23.20-1build1 amd64 p11-glue proxy and trust modules
ii packagekit 1.1.13-2ubuntu1 amd64 Provides a package management service
ii packagekit-tools 1.1.13-2ubuntu1 amd64 Provides PackageKit command-line tools
ii parted 3.3-4 amd64 disk partition manipulator
ii passwd 1:4.8.1-1ubuntu5.20.04 amd64 change and administer password and group data
ii patch 2.7.6-6 amd64 Apply a diff file to an original
ii pci.ids 0.0-2020.03.20-1 all PCI ID Repository
ii pciutils 1:3.6.4-1 amd64 PCI utilities
ii pcmciautils 018-11 amd64 PCMCIA utilities for Linux 2.6
ii perl 5.30.0-9build1 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.30.0-9build1 amd64 minimal Perl system
ii perl-modules-5.30 5.30.0-9build1 all Core Perl modules
ii perl-openssl-defaults 4 amd64 version compatibility baseline for Perl OpenSSL packages
ii php-common 2:76+ubuntu20.04.1+deb.sury.org+9 all Common files for PHP packages
ii php-pear 1:1.10.9+submodules+notgz-1 all PEAR Base System
ii php7.1-cli 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 command-line interpreter for the PHP scripting language
ii php7.1-common 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 documentation, examples and common module for PHP
ii php7.1-curl 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 CURL module for PHP
ii php7.1-gd 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 GD module for PHP
ii php7.1-intl 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 Internationalisation module for PHP
ii php7.1-json 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 JSON module for PHP
ii php7.1-mbstring 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 MBSTRING module for PHP
ii php7.1-mcrypt 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 libmcrypt module for PHP
ii php7.1-mysql 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 MySQL module for PHP
ii php7.1-opcache 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 Zend OpCache module for PHP
ii php7.1-readline 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 readline module for PHP
ii php7.1-sqlite3 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 SQLite3 module for PHP
ii php7.1-xml 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 DOM, SimpleXML, WDDX, XML, and XSL module for PHP
ii php7.1-xmlrpc 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 XMLRPC-EPI module for PHP
ii php7.1-zip 7.1.33-16+ubuntu20.04.1+deb.sury.org+1 amd64 Zip module for PHP
ii php7.2 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 all server-side, HTML-embedded scripting language (metapackage)
ii php7.2-cli 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 command-line interpreter for the PHP scripting language
ii php7.2-common 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 documentation, examples and common module for PHP
ii php7.2-curl 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 CURL module for PHP
ii php7.2-dev 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 Files for PHP7.2 module development
ii php7.2-gd 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 GD module for PHP
ii php7.2-intl 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 Internationalisation module for PHP
ii php7.2-json 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 JSON module for PHP
ii php7.2-mbstring 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 MBSTRING module for PHP
ii php7.2-mysql 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 MySQL module for PHP
ii php7.2-opcache 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 Zend OpCache module for PHP
ii php7.2-readline 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 readline module for PHP
ii php7.2-sqlite3 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 SQLite3 module for PHP
ii php7.2-xml 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 DOM, SimpleXML, WDDX, XML, and XSL module for PHP
ii php7.2-xmlrpc 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 XMLRPC-EPI module for PHP
ii php7.2-zip 7.2.32-1+ubuntu20.04.1+deb.sury.org+1 amd64 Zip module for PHP
ii pinentry-curses 1.1.0-3build1 amd64 curses-based PIN or pass-phrase entry dialog for GnuPG
ii pinentry-gnome3 1.1.0-3build1 amd64 GNOME 3 PIN or pass-phrase entry dialog for GnuPG
ii pkg-config 0.29.1-0ubuntu4 amd64 manage compile and link flags for libraries
ii pkg-php-tools 1.38 all various packaging tools and scripts for PHP packages
ii plymouth 0.9.4git20200323-0ubuntu6 amd64 boot animation, logger and I/O multiplexer
ii plymouth-label 0.9.4git20200323-0ubuntu6 amd64 boot animation, logger and I/O multiplexer - label control
ii plymouth-theme-spinner 0.9.4git20200323-0ubuntu6 amd64 boot animation, logger and I/O multiplexer - spinner theme
ii plymouth-theme-ubuntu-text 0.9.4git20200323-0ubuntu6 amd64 boot animation, logger and I/O multiplexer - ubuntu text theme
ii po-debconf 1.0.21 all tool for managing templates file translations with gettext
ii policykit-1 0.105-26ubuntu1 amd64 framework for managing administrative policies and privileges
ii policykit-desktop-privileges 0.21 all run common desktop actions without password
ii poppler-data 0.4.9-2 all encoding data for the poppler PDF rendering library
ii poppler-utils 0.86.1-0ubuntu1 amd64 PDF utilities (based on Poppler)
ii popularity-contest 1.69ubuntu1 all Vote for your favourite packages automatically
ii powermgmt-base 1.36 all common utils for power management
ii ppp 2.4.7-2+4.1ubuntu5 amd64 Point-to-Point Protocol (PPP) - daemon
ii pptp-linux 1.10.0-1build1 amd64 Point-to-Point Tunneling Protocol (PPTP) Client
ii printer-driver-brlaser 6-1build1 amd64 printer driver for (some) Brother laser printers
ii printer-driver-c2esp 27-6 amd64 printer driver for Kodak ESP AiO color inkjet Series
ii printer-driver-foo2zjs 20171202dfsg0-4 amd64 printer driver for ZjStream-based printers
ii printer-driver-foo2zzjs-common 20171202dfsg0-4 all printer driver for ZjStream-based printers - common files
ii printer-driver-hpcups 3.20.3+dfsg0-2 amd64 HP Linux Printing and Imaging - CUPS Raster driver (hpcups)
ii printer-driver-m2300w 0.51-14 amd64 printer driver for Minolta magicolor 2300W/2400W color laser printers
ii printer-driver-min12xxw 0.0.9-11 amd64 printer driver for KonicaMinolta PagePro 1[234]xxW
ii printer-driver-pnm2ppm 1.13+nondbs-0ubuntu6 amd64 printer driver for HP-GDI printers
ii printer-driver-postscript-hp 3.20.3+dfsg0-2 amd64 HP Printers PostScript Descriptions
ii printer-driver-ptouch 1.4.2-3 amd64 printer driver Brother P-touch label printers
ii printer-driver-pxljr 1.4+repack0-5 amd64 printer driver for HP Color LaserJet 35xx/36xx
ii printer-driver-sag-gdi 0.1-7 all printer driver for Ricoh Aficio SP 1000s/SP 1100s
ii printer-driver-splix 2.0.0+svn315-7fakesync1build1 amd64 Driver for Samsung and Xerox SPL2 and SPLc laser printers
ii procps 2:3.3.16-1ubuntu2 amd64 /proc file system utilities
ii psmisc 23.3-1 amd64 utilities that use the proc file system
ii publicsuffix 20200303.0012-1 all accurate, machine-readable list of domain name suffixes
ii pulseaudio 1:13.99.1-1ubuntu3.5 amd64 PulseAudio sound server
ii pulseaudio-module-bluetooth 1:13.99.1-1ubuntu3.5 amd64 Bluetooth module for PulseAudio sound server
ii pulseaudio-utils 1:13.99.1-1ubuntu3.5 amd64 Command line tools for the PulseAudio sound server
ii python3-apt-common 2.0.0ubuntu0.20.04.1 all Python interface to libapt-pkg (locales)
ii python3 3.8.2-0ubuntu2 amd64 interactive high-level object-oriented language (default python3 version)
ii python3-apport 2.20.11-0ubuntu27.4 all Python 3 library for Apport crash report handling
ii python3-apt 2.0.0ubuntu0.20.04.1 amd64 Python 3 interface to libapt-pkg
ii python3-aptdaemon 1.1.1+bzr982-0ubuntu32.1 all Python 3 module for the server and client of aptdaemon
ii python3-aptdaemon gtk3widgets 1.1.1+bzr982-0ubuntu32.1 all Python 3 GTK+ 3 widgets to run an aptdaemon client
ii python3-bcrypt 3.1.7-2ubuntu1 amd64 password hashing library for Python 3
ii python3-blinker 1.4+dfsg1-0.3ubuntu1 all fast, simple object-to-object and broadcast signaling library
ii python3-brlapi 6.0+dfsg-4ubuntu6 amd64 Braille display access via BRLTTY - Python3 bindings
ii python3-cairo 1.16.2-2ubuntu2 amd64 Python3 bindings for the Cairo vector graphics library
ii python3-certifi 2019.11.28-1 all root certificates for validating SSL certs and verifying TLS hosts (python3)

```

```

ii python3-cffi-backend 1.14.0-1build1 amd64 Foreign Function Interface for Python 3 calling C code - runtime
ii python3-chardet 3.0.4-4build1 all universal character encoding detector for Python3
ii python3-click 7.0-3 all Wrapper around optparse for command line utilities - Python 3.x
ii python3-colorama 0.4.3-1build1 all Cross-platform colored terminal text in Python - Python 3.x
ii python3-commandnotfound 20.04.2 all Python 3 bindings for command-not-found.
ii python3-crypto 2.6.1-13ubuntu2 amd64 cryptographic algorithms and protocols for Python 3
ii python3-cryptography 2.8-3 amd64 Python library exposing cryptographic recipes and primitives (Python 3)
ii python3-cups 1.9.73-3build1 amd64 Python3 bindings for CUPS
ii python3-cupshelpers 1.5.12-0ubuntu1 all Python utility modules around the CUPS printing system
ii python3-dateutil 2.7.3-3ubuntu1 all powerful extensions to the standard Python 3 datetime module
ii python3-dbus 1.2.16-1build1 amd64 simple interprocess messaging system (Python 3 interface)
ii python3-debconf 1.5.73 all interact with debconf from Python 3
ii python3-debian 0.1.36ubuntu1 all Python 3 modules to work with Debian-related data formats
ii python3-defer 1.0.6-2.1 all Small framework for asynchronous programming (Python 3)
ii python3-distro 1.4.0-1 all Linux OS platform information API
ii python3-distro-info 0.23ubuntu1 all information about distributions' releases (Python 3 module)
ii python3-distupgrade 1:20.04.23 all manage release upgrades
ii python3-dnspython 1.16.0-1build1 all DNS toolkit for Python 3
ii python3-entrypoints 0.3-2ubuntu1 all Discover and load entry points from installed packages (Python 3)
ii python3-fasteners 0.14.1-2 all provides useful locks - Python 3.x
ii python3-future 0.18.2-2 all Clean single-source support for Python 3 and 2 - Python 3.x
ii python3-gdbm 3.8.2-1ubuntu1 amd64 GNU dbm database support for Python 3.x
ii python3-gi 3.36.0-1 amd64 Python 3 bindings for gobject-introspection libraries
ii python3-gi-cairo 3.36.0-1 amd64 Python 3 Cairo bindings for the GObject library
ii python3-gpg 1.13.1-7ubuntu2 amd64 Python interface to the GPGME GnuPG encryption library (Python 3)
ii python3-httplib2 0.14.0-1ubuntu1 all comprehensive HTTP client library written for Python3
ii python3-ibus-1.0 1.5.22-2ubuntu2.1 all Intelligent Input Bus - introspection overrides for Python (Python 3)
ii python3-idna 2.8-1 all Python IDNA2008 (RFC 5891) handling (Python 3)
ii python3-jwt 1.7.1-2ubuntu2 all Python 3 implementation of JSON Web Token
ii python3-keyring 18.0.1-2ubuntu1 all store and access your passwords safely - Python 3 version of the package
ii python3-launchpadlib 1.10.13-1 all Launchpad web services client library (Python 3)
ii python3-lazr.restfulclient 0.14.2-2build1 all client for lazr.restful-based web services (Python 3)
ii python3-lazr.uri 1.0.3-4build1 all library for parsing, manipulating, and generating URIs
ii python3-ldb 2:2.0.10-0ubuntu0.20.04.1 amd64 Python 3 bindings for LDB
ii python3-lib2to3 3.8.2-1ubuntu1 all Interactive high-level object-oriented language (lib2to3)
ii python3-lockfile 1:0.12.2-2ubuntu2 all file locking library for Python - Python 3 library
ii python3-louis 3.12.0-3 all Python bindings for liblouis
ii python3-macaroonbakery 1.3.1-1 all Higher-level macaroon operations for Python 3
ii python3-mako 1.1.0+ds1-1ubuntu2 all fast and lightweight templating for the Python 3 platform
ii python3-markdown 3.1.1-3 all text-to-HTML conversion library/tool (Python 3 version)
ii python3-markupsafe 1.1.0-1build2 amd64 HTML/XHTML/XML string library for Python 3
ii python3-minimal 3.8.2-0ubuntu2 amd64 minimal subset of the Python language (default python3 version)
ii python3-monotonic 1.5-0ubuntu2 all implementation of time.monotonic() - Python 3.x
ii python3-nacl 1.3.0-5 amd64 Python bindings to libsodium (Python 3)
ii python3-netifaces 0.10.4-1ubuntu4 amd64 portable network interface information - Python 3.x
ii python3-oauthlib 3.1.0-1ubuntu2 all generic, spec-compliant implementation of OAuth for Python3
ii python3-olefile 0.46-2 all Python module to read/write MS OLE2 files
ii python3-packaging 20.3-1 all core utilities for python3 packages
ii python3-paramiko 2.6.0-2 all Make ssh v2 connections (Python 3)
ii python3-pexpect 4.6.0-1build1 all Python 3 module for automating interactive applications
ii python3-pil 7.0.0-4ubuntu0.1 amd64 Python Imaging Library (Python3)
ii python3-pkg-resources 45.2.0-1 all Package Discovery and Resource Access using pkg_resources
ii python3-problem-report 2.20.11-0ubuntu27.4 all Python 3 library to handle problem reports
ii python3-protobuf 3.6.1.3-2ubuntu5 amd64 Python 3 bindings for protocol buffers
ii python3-ptyprocess 0.6.0-1ubuntu1 all Run a subprocess in a pseudo terminal from Python 3
ii python3-pyatspi 2.36.0-1 all Assistive Technology Service Provider Interface - Python3 bindings
ii python3-pygments 2.3.1+dfsg-1ubuntu2 all syntax highlighting package written in Python 3
ii python3-pymacaroons 0.13.0-3 all Macaroon library for Python 3
ii python3-pyparsing 2.4.6-1 all alternative to creating and executing simple grammars - Python 3.x
ii python3-renderpm 3.5.34-1ubuntu1 amd64 python low level render interface
ii python3-reportlab 3.5.34-1ubuntu1 all ReportLab library to create PDF documents using Python3
ii python3-reportlab-accel 3.5.34-1ubuntu1 amd64 C coded extension accelerator for the ReportLab Toolkit
ii python3-requests 2.22.0-2ubuntu1 all elegant and simple HTTP library for Python3, built for human beings
ii python3-requests-unixsocket 0.2.0-2 all Use requests to talk HTTP via a UNIX domain socket - Python 3.x
ii python3-rfc3339 1.1-2 all parser and generator of RFC 3339-compliant timestamps (Python 3)
ii python3-samba 2:4.11.6+dfsg-1ubuntu1.3 amd64 Python 3 bindings for Samba
ii python3-secretstorage 2.3.1-2ubuntu1 all Python module for storing secrets - Python 3.x version
ii python3-simplejson 3.16.0-2ubuntu2 amd64 simple, fast, extensible JSON encoder/decoder for Python 3.x
ii python3-six 1.14.0-2 all Python 2 and 3 compatibility library (Python 3 interface)
ii python3-software-properties 0.98.9.1 all manage the repositories that you install software from
ii python3-speechd 0.9.1-4 all Python interface to Speech Dispatcher
ii python3-systemd 234-3build2 amd64 Python 3 bindings for systemd
ii python3-talloc 2.3.0-3ubuntu1 amd64 hierarchical pool based memory allocator - Python3 bindings
ii python3-tdb 1.4.2-3build1 amd64 Python3 bindings for TDB
ii python3-tz 2019.3-1 all Python3 version of the Olson timezone database
ii python3-uno 1:6.4.4-0ubuntu0.20.04.1 amd64 Python-UNO bridge
ii python3-update-manager 1:20.04.10.1 all python 3.x module for update-manager
ii python3-urllib3 1.25.8-2 all HTTP library with thread-safe connection pooling for Python3
ii python3-wadllib 1.3.3-3build1 all Python 3 library for navigating WADL files
ii python3-xdg 0.26-1ubuntu1 all Python 3 library to access freedesktop.org standards
ii python3-xkit 0.5.0ubuntu4 all library for the manipulation of xorg.conf files (Python 3)
ii python3-yaml 5.3.1-1 amd64 YAML parser and emitter for Python3
ii python3.8 3.8.2-1ubuntu1.2 amd64 Interactive high-level object-oriented language (version 3.8)
ii python3.8-minimal 3.8.2-1ubuntu1.2 amd64 Minimal subset of the Python language (version 3.8)
ii readline-common 8.0-4 all GNU readline and history libraries, common files
ii remmina 1.4.2+dfsg-1ubuntu1 amd64 GTK+ Remote Desktop Client
ii remmina-common 1.4.2+dfsg-1ubuntu1 all Common files for Remmina
ii remmina-plugin-rdp 1.4.2+dfsg-1ubuntu1 amd64 RDP plugin for Remmina
ii remmina-plugin-secret 1.4.2+dfsg-1ubuntu1 amd64 Secret plugin for Remmina
ii remmina-plugin-vnc 1.4.2+dfsg-1ubuntu1 amd64 VNC plugin for Remmina
ii rfkill 2.34-0.1ubuntu9 amd64 tool for enabling and disabling wireless devices
ii rhythmbox 3.4.4-1ubuntu2 amd64 music player and organizer for GNOME
ii rhythmbox-data 3.4.4-1ubuntu2 all data files for rhythmbox
ii rhythmbox-plugin-alternative-toolbar 0.19.3-1 all Enhanced play controls and interface for Rhythmbox
ii rhythmbox-plugins 3.4.4-1ubuntu2 amd64 plugins for rhythmbox music player
ii rsync 3.1.3-8 amd64 fast, versatile, remote (and local) file-copying tool
ii rsyslog 8.2001.0-1ubuntu1 amd64 reliable system and kernel logging daemon
ii rtkit 0.12-4 amd64 Realtime Policy and Watchdog Daemon
ii rygel 0.38.3-1ubuntu1 amd64 GNOME UPnP/DLNA services

```

```
ii samba 2:4.11.6+dfsg-0ubuntu1.3 amd64 SMB/CIFS file, print, and login server for Unix
ii samba-common 2:4.11.6+dfsg-0ubuntu1.3 all common files used by both the Samba server and client
ii samba-common-bin 2:4.11.6+dfsg-0ubuntu1.3 amd64 Samba common files used by both the server and the client
ii samba-dsdb-modules 2:4.11.6+dfsg-0ubuntu1.3 amd64 Samba Directory Services Database
ii samba-libs 2:4.11.6+dfsg-0ubuntu1.3 amd64 Samba core libraries
ii samba-vfs-modules 2:4.11.6+dfsg-0ubuntu1.3 amd64 Samba Virtual FileSystem plugins
ii sane-utils 1.0.29-0ubuntu5 amd64 API library for scanners -- utilities
ii sbsigntool 0.9.2-2ubuntu1 amd64 Tools to manipulate signatures on UEFI binaries and drivers
ii seahorse 3.36-1 amd64 GNOME front end for GnuPG
ii secureboot-db 1.5 amd64 Secure Boot updates for DB and DBX
ii sed 4.7-1 amd64 GNU stream editor for filtering/transforming text
ii sensible-utils 0.0.12+nmu1 all Utilities for sensible alternative selection
ii session-migration 0.3.5 amd64 Tool to migrate in user session settings
ii sgml-base 1.29.1 all SGML infrastructure and SGML catalog file support
ii sgml-data 2.0.11 all common SGML and XML data
ii shared-mime-info 1.15-1 amd64 FreeDesktop.org shared MIME database and spec
ii shotwell 0.30.10-0ubuntu0.1 amd64 digital photo organizer
ii shotwell-common 0.30.10-0ubuntu0.1 all digital photo organizer - common files
ii shtool 2.0.8-10 all portable shell tool from the GNU project
ii simple-scan 3.36.0-0ubuntu1 amd64 Simple Scanning Utility
ii snapd 2.45.1+20.04.2 amd64 Daemon and tooling that enable snap packages
ii socat 1.7.3.3-2 amd64 multipurpose relay for bidirectional data transfer
ii software-properties-common 0.98.9.1 all manage the repositories that you install software from (common)
ii software-properties-gtk 0.98.9.1 all manage the repositories that you install software from (gtk)
ii sound-icons 0.1-7 all Sounds for speech enabled applications
ii sound-theme-freedesktop 0.8-2ubuntu1 all freedesktop.org sound theme
ii speech-dispatcher 0.9.1-4 amd64 Common interface to speech synthesizers
ii speech-dispatcher-audio-plugins 0.9.1-4 amd64 Speech Dispatcher: Audio output plugins
ii speech-dispatcher-espeak-ng 0.9.1-4 amd64 Speech Dispatcher: Espeak-ng output module
ii spice-vdagent 0.19.0-2 amd64 Spice agent for Linux
ii squashfs-tools 1:4.4-1 amd64 Tool to create and append to squashfs filesystems
ii ssh 1:8.2p1-4ubuntu0.1 all secure shell client and server (metapackage)
ii ssh-import-id 5.10-0ubuntu1 all securely retrieve an SSH public key and install it locally
ii ssl-cert 1.0.39 all simple debconf wrapper for OpenSSL
ii strace 5.5-3ubunt1 amd64 System call tracer
ii sudo 1.8.31-1ubunt1 amd64 Provide limited super user privileges to specific users
ii switcheroo-control 2.1-1 amd64 D-Bus service to check the availability of dual-GPU
ii syslinux 3:6.04~git20190206.bf6db5b4+dfsg1-2 amd64 collection of bootloaders (DOS FAT and NTFS bootloader)
ii syslinux-common 3:6.04~git20190206.bf6db5b4+dfsg1-2 all collection of bootloaders (common)
ii syslinux-legacy 2:3.63+dfsg-2ubuntu9 amd64 Bootloader for Linux/i386 using MS-DOS floppies
ii system-config-printer 1.5.12-0ubunt1 all graphical interface to configure the printing system
ii system-config-printer-common 1.5.12-0ubunt1 all backend and the translation files for system-config-printer
ii system-config-printer-udev 1.5.12-0ubunt1 amd64 Utilities to detect and configure printers automatically
ii systemd 245.4-4ubunt3.2 amd64 system and service manager
ii systemd-sysv 245.4-4ubunt3.2 amd64 system and service manager - SysV links
ii systemd-timesyncd 245.4-4ubunt3.2 amd64 minimalistic service to synchronize local time with NTP servers
ii sysvinit-utils 2.96-2.1ubunt1 amd64 System-V-like utilities
ii tar 1.30+dfsg-7 amd64 GNU version of the tar archiving utility
ii tcpdump 4.9.3-4 amd64 command-line network traffic analyzer
ii tdb-tools 1.4.2-3build1 amd64 Trivial Database - bundled binaries
ii telnet 0.17-41.2build1 amd64 basic telnet client
ii thermald 1.9.1-1ubunt0.2 amd64 Thermal monitoring and controlling daemon
ii thunderbird 1:68.10.0+build1-0ubunt0.20.04.1 amd64 Email, RSS and newsgroup client with integrated spam filter
ii thunderbird-gnome-support 1:68.10.0+build1-0ubunt0.20.04.1 amd64 Email, RSS and newsgroup client - GNOME support
ii thunderbird-locale-de 1:68.10.0+build1-0ubunt0.20.04.1 amd64 German language pack for Thunderbird
ii thunderbird-locale-en 1:68.10.0+build1-0ubunt0.20.04.1 amd64 English language pack for Thunderbird
ii thunderbird-locale-en-gb 1:68.10.0+build1-0ubunt0.20.04.1 all Transitional English language pack for Thunderbird
ii thunderbird-locale-en-us 1:68.10.0+build1-0ubunt0.20.04.1 all Transitional English language pack for Thunderbird
ii time 1.7-25.1build1 amd64 GNU time program for measuring CPU resource usage
ii totem 3.34.1-2ubunt2 amd64 Simple media player for the GNOME desktop based on GStreamer
ii totem-common 3.34.1-2ubunt2 all Data files for the Totem media player
ii totem-plugins 3.34.1-2ubunt2 amd64 Plugins for the Totem media player
ii tpm-udev 0.4 all udev rules for TPM modules
ii tracker 2.3.4-1 amd64 metadata database, indexer and search tool
ii tracker-extract 2.3.3-2 amd64 metadata database, indexer and search tool - metadata extractors
ii tracker-miner-fs 2.3.3-2 amd64 metadata database, indexer and search tool - filesystem indexer
ii transmission-common 2.94-2ubunt3 all lightweight BitTorrent client (common files)
ii transmission-gtk 2.94-2ubunt3 amd64 lightweight BitTorrent client (GTK+ interface)
ii tzdata 2020a-0ubunt0.20.04 all time zone and daylight-saving time data
ii ubuntu-advantage-tools 20.3 amd64 management tools for Ubuntu Advantage
ii ubuntu-desktop 1.450.1 amd64 The Ubuntu desktop system
ii ubuntu-desktop-minimal 1.450.1 amd64 The Ubuntu desktop minimal system
ii ubuntu-docs 20.04.3 all Ubuntu Desktop Guide
ii ubuntu-drivers-common 1:0.8.4-0.20.04.3 amd64 Detect and install additional Ubuntu driver packages
ii ubuntu-keyring 2020.02.11.2 all GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.450.1 amd64 Minimal core of Ubuntu
ii ubuntu-mono 19.04-0ubunt3 all Ubuntu Mono Icon theme
ii ubuntu-release-upgrader-core 1:20.04.23 all manage release upgrades
ii ubuntu-release-upgrader-gtk 1:20.04.23 all manage release upgrades
ii ubuntu-report 1.6.1 amd64 Report hardware and other collected metrics
ii ubuntu-session 3.36.0-2ubunt1 all Ubuntu session with GNOME Shell
ii ubuntu-settings 20.04.5 all default settings for the Ubuntu desktop
ii ubuntu-standard 1.450.1 amd64 The Ubuntu standard system
ii ubuntu-wallpapers 20.04.2-0ubunt1 all Ubuntu Wallpapers
ii ubuntu-wallpapers-focal 20.04.2-0ubunt1 all Ubuntu 20.04 Wallpapers
ii ucf 3.0038+nmu1 all Update Configuration File(s): preserve user changes to config files
ii udev 245.4-4ubunt3.2 amd64 /dev/ and hotplug management daemon
ii udisks2 2.8.4-1ubunt1 amd64 D-Bus service to access and manipulate storage devices
ii ufw 0.36-6 all program for managing a Netfilter firewall
ii unattended-upgrades 2.3 all automatic installation of security upgrades
ii uno-libs-private 1:6.4.4-0ubunt0.20.04.1 amd64 LibreOffice UNO runtime environment -- private libraries used by public ones
ii unzip 6.0-25ubunt1 amd64 De-archiver for .zip files
ii update-inetd 4.50 all inetd configuration file updater
ii update-manager 1:20.04.10.1 all GNOME application that manages apt updates
ii update-manager-core 1:20.04.10.1 all manage release upgrades
ii update-notifier 3.192.30 amd64 Daemon which notifies about package updates
ii update-notifier-common 3.192.30 all Files shared between update-notifier and other packages
ii upower 0.99.11-1ubild2 amd64 abstraction for power management
ii ure 1:6.4.4-0ubunt0.20.04.1 amd64 LibreOffice UNO runtime environment
```

```

ii usb-creator-common 0.3.7 amd64 create a startup disk using a CD or disc image (common files)
ii usb-creator-gtk 0.3.7 amd64 create a startup disk using a CD or disc image (for GNOME)
ii usb-modeswitch 2.5.2+repack0~2ubuntu3 amd64 mode switching tool for controlling "flip flop" USB devices
ii usb-modeswitch-data 20191128-3 all mode switching data for usb-modeswitch
ii usb.ids 2020.03.19-1 all USB ID Repository
ii usbmuxd 1.1.1~git20191130.9af2b12-1 amd64 USB multiplexor daemon for iPhone and iPod Touch devices
ii usbutils 1:0.12-2 amd64 Linux USB utilities
ii util-linux 2.34-0.1ubuntu9 amd64 miscellaneous system utilities
ii uuid-runtime 2.34-0.1ubuntu9 amd64 runtime components for the Universally Unique ID library
ii vim-common 2:8.1.2269-1ubuntu5 all Vi IMproved - Common files
ii vim-tiny 2:8.1.2269-1ubuntu5 amd64 Vi IMproved - enhanced vi editor - compact version
ii vino 3.22.0-5ubuntu2 amd64 VNC server for GNOME
ii wamerican 2018.04.16-1 all American English dictionary words for /usr/share/dict
ii wbritish 2018.04.16-1 all British English dictionary words for /usr/share/dict
ii wget 1.20.3-1ubuntu1 amd64 retrieves files from the web
ii whiptail 0.52.21-4ubuntu2 amd64 Displays user-friendly dialog boxes from shell scripts
ii whoopsie 0.2.69 amd64 Ubuntu error tracker submission
ii whoopsie-preferences 22 amd64 System preferences for error reporting
ii wireless-regdb 2018.05.09-0ubuntu1 all wireless regulatory database
ii wireless-tools 30~pre9-13ubuntu1 amd64 Tools for manipulating Linux Wireless Extensions
ii wngerman 20161207-7 all New German orthography wordlist
ii wogerman 1:2-35 all Traditional German wordlist
ii wpasupplicant 2:2.9-1ubuntu4.1 amd64 client support for WPA and WPA2 (IEEE 802.11i)
ii wswiss 20161207-7 all Swiss (German) orthography wordlist
ii x11-apps 7.7+8 amd64 X applications
ii x11-common 1:7.7+19ubuntu14 all X Window System (X.Org) infrastructure
ii x11-session-utils 7.7+4 amd64 X session utilities
ii x11-utils 7.7+5 amd64 X11 utilities
ii x11-xkb-utils 7.7+5 amd64 X11 XKB utilities
ii x11-xserver-utils 7.7+8 amd64 X server utilities
ii xauth 1:1.1-0ubuntu1 amd64 X authentication utility
ii xbitmaps 1.1.1-2 all Base X bitmaps
ii xbrlapi 6.0+dfsg-4ubuntu6 amd64 Access software for a blind person using a braille display - xbrlapi
ii xcursor-themes 1.0.6-0ubuntu1 all Base X cursor themes
ii xdg-dbus-proxy 0.1.2-1 amd64 filtering D-Bus proxy
ii xdg-desktop-portal 1.6.0-1 amd64 desktop integration portal for Flatpak and Snap
ii xdg-desktop-portal-gtk 1.6.0-1build1 amd64 GTK+/GNOME portal backend for xdg-desktop-portal
ii xdg-user-dirs 0.17-2ubuntu1 amd64 tool to manage well known user directories
ii xdg-user-dirs-gtk 0.10-3 amd64 tool to manage well known user directories (Gtk extension)
ii xdg-utils 1.1.3-2ubuntu1 all desktop integration utilities from freedesktop.org
ii xfonts-base 1:1.0.5 all standard fonts for X
ii xfonts-encodings 1:1.0.5-0ubuntu1 all Encodings for X.Org fonts
ii xfonts-scalable 1:1.0.3-1.1 all scalable fonts for X
ii xfonts-utils 1:7.7+6 amd64 X Window System font utility programs
ii xinit 1.4.1-0ubuntu2 amd64 X server initialisation tool
ii xinput 1.6.3-1 amd64 Runtime configuration and test of XInput devices
ii xkb-data 2.29-2 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.18+nmui all XML infrastructure and XML catalog file support
ii xorg 1:7.7+19ubuntu14 amd64 X.Org X Window System
ii xorg-docs-core 1:1.7.1-1.1 all Core documentation for the X.Org X Window System
ii xserver-common 2:1.20.8-2ubuntu2.2 all common files used by various X servers
ii xserver-xephyr 2:1.20.8-2ubuntu2.2 amd64 nested X server
ii xserver-xorg 1:7.7+19ubuntu14 amd64 X.Org X server
ii xserver-xorg-core 2:1.20.8-2ubuntu2.2 amd64 Xorg X server - core server
ii xserver-xorg-input-all 1:7.7+19ubuntu14 amd64 X.Org X server -- input driver metapackage
ii xserver-xorg-input-libinput 0.29.0-1 amd64 X.Org X server -- libinput input driver
ii xserver-xorg-input-wacom 1:0.39.0-0ubuntu1 amd64 X.Org X server -- Wacom input driver
ii xserver-xorg-legacy 2:1.20.8-2ubuntu2.2 amd64 setuid root Xorg server wrapper
ii xserver-xorg-video-all 1:7.7+19ubuntu14 amd64 X.Org X server -- output driver metapackage
ii xserver-xorg-video-amdgpu 19.1.0-1 amd64 X.Org X server -- AMDGPU display driver
ii xserver-xorg-video-ati 1:19.1.0-1 amd64 X.Org X server -- AMD/ATI display driver wrapper
ii xserver-xorg-video-fbdev 1:0.5.0-1ubuntu1 amd64 X.Org X server -- fbdev display driver
ii xserver-xorg-video-intel 2:2.99.917+git20200226-1 amd64 X.Org X server -- Intel i8xx, i9xx display driver
ii xserver-xorg-video-nouveau 1:1.0.16-1 amd64 X.Org X server -- Nouveau display driver
ii xserver-xorg-video-qxl 0.1.5+git20200331-1 amd64 X.Org X server -- QXL display driver
ii xserver-xorg-video-radeon 1:19.1.0-1 amd64 X.Org X server -- AMD/ATI Radeon display driver
ii xserver-xorg-video-vesa 1:2.4.0-2 amd64 X.Org X server -- VESA display driver
ii xserver-xorg-video-vmware 1:13.3.0-3 amd64 X.Org X server -- VMware display driver
ii xul-ext-ubufox 3.4-0ubuntu1 3.4-0ubuntu1 all Ubuntu modifications for Firefox
ii xwayland 2:1.20.8-2ubuntu2.2 amd64 Xwayland X server
ii xxd 2:8.1.2269-1ubuntu5 amd64 tool to make (or reverse) a hex dump
ii xz-utils 5.2.4-1 amd64 XZ-format compression utilities
ii yaru-theme-gnome-shell 20.04.7 all Yaru GNOME Shell desktop theme from the Ubuntu Community
ii yaru-theme-gtk 20.04.7 all Yaru GTK theme from the Ubuntu Community
ii yaru-theme-icon 20.04.7 all Yaru icon theme from the Ubuntu Community
ii yaru-theme-sound 20.04.7 all Yaru sound theme from the Ubuntu Community
ii yelp 3.36.0-1 amd64 Help browser for GNOME
ii yelp-xsl 3.36.0-1 all XSL stylesheets for the yelp help browser
ii zenity 3.32.0-5 amd64 Display graphical dialog boxes from shell scripts
ii zenity-common 3.32.0-5 all Display graphical dialog boxes from shell scripts (common files)
ii zip 3.0-11build1 amd64 Archiver for .zip files
ii zlib1g 1:1.2.11.dfsg-2ubuntu1 amd64 compression library - runtime

```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege**Synopsis**

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialled checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

Nessus was able to log into the remote host, however this credential did not have sufficient privileges for all planned checks :

```
User: 'silky'  
Port: 22  
Proto: SSH  
Method: password
```

See the output of the following plugin for details :

```
Plugin ID : 102094  
Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided**Synopsis**

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

Nessus was able to log in to the remote host via the following :

```
User: 'silky'
Port: 22
Proto: SSH
Method: password
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot system boot 5.4.0-42-generic Tue Nov 4 06:43 still running
reboot system boot 5.4.0-42-generic Mon Nov 3 07:50 still running
reboot system boot 5.4.0-42-generic Fri Jul 31 09:49 - 10:19 (00:29)
reboot system boot 5.4.0-42-generic Thu Jul 30 12:19 - 12:32 (00:13)
reboot system boot 5.4.0-42-generic Thu Jul 30 03:19 - 04:45 (01:25)
reboot system boot 5.4.0-42-generic Wed Jul 29 06:28 - 07:10 (00:42)
reboot system boot 5.4.0-42-generic Wed Jul 29 04:18 - 06:19 (02:01)
reboot system boot 5.4.0-42-generic Wed Jul 29 00:45 - 04:17 (03:32)
reboot system boot 5.4.0-42-generic Tue Jul 28 23:35 - 00:45 (01:10)

wtmp beginnt Tue Jul 28 23:35:03 2020
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.22.169.33 to 10.22.169.205 :  
10.22.169.33  
10.22.169.205
```

Hop Count: 1

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://xz.tukaani.org/xz-utils/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of XZ Utils:

```
Path : liblzma5 5.2.4-1 (via package manager)  
Version : 5.2.4  
Managed by OS : True
```

```
Path : xz-utils 5.2.4-1 (via package manager)  
Version : 5.2.4  
Managed by OS : True
```

193128 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server regression (USN-6721-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6721-2 advisory.

USN-6721-1 fixed vulnerabilities in X.Org X Server. That fix was incomplete resulting in a regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6721-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6721-2

Plugin Information

Published: 2024/04/10, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.17
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.17
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.17
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.17
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.17

214325 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : rsync regression (USN-7206-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7206-2 advisory.

USN-7206-1 fixed vulnerabilities in rsync. The update introduced a regression in rsync. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7206-2>

Solution

Update the affected rsync package.

Risk Factor

None

References

XREF USN:7206-2

Plugin Information

Published: 2025/01/17, Modified: 2025/01/17

Plugin Output

tcp/0

- Installed package : rsync_3.1.3-8
- Fixed package : rsync_3.1.3-8ubuntu0.9

179597 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : OpenSSH update (USN-6279-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6279-1 advisory.

It was discovered that OpenSSH has an observable discrepancy leading to an information leak in the algorithm negotiation. This update mitigates the issue by tweaking the client hostkey preference ordering algorithm to prefer the default ordering if the user has a key that matches the best-preference default algorithm.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6279-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6279-1

Plugin Information

Published: 2023/08/09, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : openssh-client_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-client_1:8.2p1-4ubuntu0.9
- Installed package : openssh-server_1:8.2p1-4ubuntu0.1

- Fixed package : openssh-server_1:8.2p1-4ubuntu0.9
- Installed package : openssh-sftp-server_1:8.2p1-4ubuntu0.1
- Fixed package : openssh-sftp-server_1:8.2p1-4ubuntu0.9
- Installed package : ssh_1:8.2p1-4ubuntu0.1
- Fixed package : ssh_1:8.2p1-4ubuntu0.9

153569 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5086-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5086-1 advisory.

Johan Almbladh discovered that the eBPF JIT implementation for IBM s390x systems in the Linux kernel miscompiled operations in some situations, allowing circumvention of the BPF verifier. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5086-1>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:5086-1

Plugin Information

Published: 2021/09/22, Modified: 2024/08/27

Plugin Output

tcp/0

NOTE: This vulnerability check contains fixes that apply to packages only available in Ubuntu ESM repositories. Access to these package security updates require an Ubuntu Pro subscription.

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-86-generic for this advisory.

168281 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : shadow regression (USN-5745-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5745-2 advisory.

USN-5745-1 fixed vulnerabilities in shadow. Unfortunately that update introduced a regression that caused useradd to behave incorrectly in Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. This update reverts the security fix pending further investigation.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5745-2>

Solution

Update the affected login, passwd and / or uidmap packages.

Risk Factor

None

References

XREF USN:5745-2

Plugin Information

Published: 2022/11/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : login_1:4.8.1-1ubuntu5.20.04
- Fixed package : login_1:4.8.1-1ubuntu5.20.04.4

- Installed package : passwd_1:4.8.1-1ubuntu5.20.04
- Fixed package : passwd_1:4.8.1-1ubuntu5.20.04.4

158258 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : snapd regression (USN-5292-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5292-4 advisory.

USN-5292-1 fixed a vulnerability in snapd. Unfortunately that update introduced a regression that could break the fish shell. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5292-4>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5292-4

Plugin Information

Published: 2022/02/22, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : snapd_2.45.1+20.04.2
- Fixed package : snapd_2.54.3+20.04.1ubuntu0.2

201126 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : CUPS regression (USN-6844-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6844-2 advisory.

USN-6844-1 fixed vulnerabilities in the CUPS package. The update lead to the discovery of a regression in CUPS with regards to how the cupsd daemon handles Listen configuration directive.

This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6844-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6844-2

Plugin Information

Published: 2024/06/28, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : cups_2.3.1-9ubuntu1.1
- Fixed package : cups_2.3.1-9ubuntu1.8
- Installed package : cups-bsd_2.3.1-9ubuntu1.1
- Fixed package : cups-bsd_2.3.1-9ubuntu1.8
- Installed package : cups-client_2.3.1-9ubuntu1.1
- Fixed package : cups-client_2.3.1-9ubuntu1.8
- Installed package : cups-common_2.3.1-9ubuntu1.1
- Fixed package : cups-common_2.3.1-9ubuntu1.8
- Installed package : cups-core-drivers_2.3.1-9ubuntu1.1
- Fixed package : cups-core-drivers_2.3.1-9ubuntu1.8
- Installed package : cups-daemon_2.3.1-9ubuntu1.1
- Fixed package : cups-daemon_2.3.1-9ubuntu1.8
- Installed package : cups-ipp-utils_2.3.1-9ubuntu1.1
- Fixed package : cups-ipp-utils_2.3.1-9ubuntu1.8
- Installed package : cups-ppdc_2.3.1-9ubuntu1.1
- Fixed package : cups-ppdc_2.3.1-9ubuntu1.8
- Installed package : cups-server-common_2.3.1-9ubuntu1.1
- Fixed package : cups-server-common_2.3.1-9ubuntu1.8
- Installed package : libcups2_2.3.1-9ubuntu1.1
- Fixed package : libcups2_2.3.1-9ubuntu1.8
- Installed package : libcurlimage2_2.3.1-9ubuntu1.1
- Fixed package : libcurlimage2_2.3.1-9ubuntu1.8

142870 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport regression (USN-4171-6)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4171-6 advisory.

USN-4171-1 fixed vulnerabilities in Apport. The update caused a regression when handling configuration files. This update fixes the problem, and also introduces further hardening measures.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4171-6>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4171-6

Plugin Information

Published: 2020/11/12, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.12
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.12
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.12
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.12

147987 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Dnsmasq regression (USN-4698-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4698-2 advisory.

USN-4698-1 fixed vulnerabilities in Dnsmasq. The updates introduced regressions in certain environments related to issues with multiple queries, and issues with retries. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4698-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4698-2

Plugin Information

Published: 2021/03/23, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : dnsmasq-base_2.80-1.1ubuntu1
- Fixed package : dnsmasq-base_2.80-1.1ubuntu1.3

146306 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox regression (USN-4717-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4717-2 advisory.

USN-4717-1 fixed vulnerabilities in Firefox. The update caused a startup hang in some circumstances. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4717-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4717-2

Plugin Information

Published: 2021/02/09, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_85.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_85.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_85.0.1+build1-0ubuntu0.20.04.1

141482 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox regressions (USN-4546-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4546-2 advisory.

USN-4546-1 fixed vulnerabilities in Firefox. The update introduced various minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4546-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4546-2

Plugin Information

Published: 2020/10/16, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_81.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_81.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_81.0.2+build1-0ubuntu0.20.04.1
```

142502 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox regressions (USN-4599-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4599-3 advisory.

USN-4599-1 and USN-4599-2 fixed vulnerabilities in Firefox. The updates introduced various minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4599-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4599-3

Plugin Information

Published: 2020/11/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_82.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_82.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_82.0.2+build1-0ubuntu0.20.04.1

142741 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode regression (USN-4628-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4628-2 advisory.

USN-4628-1 provided updated Intel Processor Microcode. Unfortunately, that update prevented certain processors in the Intel Tiger Lake family from booting successfully. This update reverts the microcode update for the Tiger Lake processor family.

Please note that the 'dis_ucode_ldr' kernel command line option can be added in the boot menu to disable microcode loading for system recovery.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4628-2>

Solution

Update the affected intel-microcode package.

Risk Factor

None

References

XREF USN:4628-2

Plugin Information

Published: 2020/11/12, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20200609.0ubuntu0.20.04.2
- Fixed package : intel-microcode_3.20201110.0ubuntu0.20.04.2

142017 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ca-certificates update (USN-4608-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4608-1 advisory.

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.44 version of the Mozilla certificate authority bundle.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4608-1>

Solution

Update the affected ca-certificates and / or ca-certificates-udeb packages.

Risk Factor

None

References

XREF USN:4608-1

Plugin Information

Published: 2020/10/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20201027ubuntu0.20.04.1

146070 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ca-certificates update (USN-4719-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4719-1 advisory.

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.46 version of the Mozilla certificate authority bundle.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4719-1>

Solution

Update the affected ca-certificates and / or ca-certificates-udeb packages.

Risk Factor

None

References

XREF USN:4719-1

Plugin Information

Published: 2021/02/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20210119~20.04.1

144709 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-apt regression (USN-4668-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4668-3 advisory.

USN-4668-1 fixed vulnerabilities in python-apt. The update caused a regression when using certain APIs with a file handle. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4668-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4668-3

Plugin Information

Published: 2021/01/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : python-apt-common_2.0.0ubuntu0.20.04.1
- Fixed package : python-apt-common_2.0.0ubuntu0.20.04.3
- Installed package : python3-apt_2.0.0ubuntu0.20.04.1
- Fixed package : python3-apt_2.0.0ubuntu0.20.04.3

144890 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils regression (USN-4649-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4649-2 advisory.

USN-4649-1 fixed vulnerabilities in xdg-utils. That update caused a regression by removing the --attach functionality in thunderbird and others applications. This update fix the problem by reverting these changes.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4649-2>

Solution

Update the affected xdg-utils package.

Risk Factor

None

References

XREF USN:4649-2

Plugin Information

Published: 2021/01/13, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : xdg-utils_1.1.3-2ubuntu1
- Fixed package : xdg-utils_1.1.3-2ubuntu1.20.04.2

176340 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ca-certificates update (USN-6105-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6105-1 advisory.

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.60 version of the Mozilla certificate authority bundle.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6105-1>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:6105-1

Plugin Information

Published: 2023/05/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20230311ubuntu0.20.04.1

168466 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : ca-certificates update (USN-5761-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5761-1 advisory.

Due to security concerns, the TrustCor certificate authority has been marked as distrusted in Mozilla's root store. This update removes the TrustCor CA certificates from the ca-certificates package.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5761-1>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5761-1

Plugin Information

Published: 2022/12/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20211016ubuntu0.20.04.1

160519 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : networkd-dispatcher regression (USN-5395-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5395-2 advisory.

USN-5395-1 fixed vulnerabilities in networkd-dispatcher. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5395-2>

Solution

Update the affected networkd-dispatcher package.

Risk Factor

None

References

XREF USN:5395-2

Plugin Information

Published: 2022/05/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : networkd-dispatcher_2.0.1-1
- Fixed package : networkd-dispatcher_2.1-2~ubuntu20.04.3

153785 - Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server regression (USN-5090-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5090-3 advisory.

USN-5090-1 fixed vulnerabilities in Apache HTTP Server. One of the upstream fixes introduced a regression in UDS URIs. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5090-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5090-3

Plugin Information

Published: 2021/09/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.6
- Installed package : apache2-bin_2.4.41-4ubuntu3

- Fixed package : apache2-bin_2.4.41-4ubuntu3.6
- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.6
- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.6

154405 - Ubuntu 18.04 LTS / 20.04 LTS : Apport vulnerability (USN-5122-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5122-1 advisory.

It was discovered that Apport could be tricked into writing core files as root into arbitrary directories in certain scenarios. A local attacker could possibly use this issue to escalate privileges. This update will cause Apport to generate all core files in the /var/lib/apport/coredump directory.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5122-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5122-1

Plugin Information

Published: 2021/10/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apport_2.20.11-0ubuntu27.4
- Fixed package : apport_2.20.11-0ubuntu27.21
- Installed package : apport-gtk_2.20.11-0ubuntu27.4
- Fixed package : apport-gtk_2.20.11-0ubuntu27.21
- Installed package : python3-apport_2.20.11-0ubuntu27.4
- Fixed package : python3-apport_2.20.11-0ubuntu27.21
- Installed package : python3-problem-report_2.20.11-0ubuntu27.4
- Fixed package : python3-problem-report_2.20.11-0ubuntu27.21

162263 - Ubuntu 18.04 LTS / 20.04 LTS : BlueZ vulnerabilities (USN-5481-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5481-1 advisory.

It was discovered that BlueZ incorrectly validated certain capabilities and lengths when handling the A2DP profile. A remote attacker could use this issue to cause BlueZ to crash, resulting in a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5481-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5481-1

Plugin Information

Published: 2022/06/15, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bluez_5.53-0ubuntu3
- Fixed package : bluez_5.53-0ubuntu3.6
- Installed package : bluez-cups_5.53-0ubuntu3
- Fixed package : bluez-cups_5.53-0ubuntu3.6
- Installed package : bluez-obexd_5.53-0ubuntu3
- Fixed package : bluez-obexd_5.53-0ubuntu3.6
- Installed package : libbluetooth3_5.53-0ubuntu3
- Fixed package : libbluetooth3_5.53-0ubuntu3.6

152830 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regression (USN-5037-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5037-2 advisory.

USN-5037-1 fixed vulnerabilities in Firefox. The update introduced a regression that caused Firefox to repeatedly prompt for a password. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5037-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5037-2

Plugin Information

Published: 2021/08/25, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_91.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_91.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_91.0.2+build1-0ubuntu0.20.04.1
```

156203 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5186-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5186-2 advisory.

USN-5186-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5186-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5186-2

Plugin Information

Published: 2021/12/20, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_95.0.1+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_95.0.1+build2-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_95.0.1+build2-0ubuntu0.20.04.1
```

159208 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5321-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5321-3 advisory.

USN-5321-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5321-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5321-3

Plugin Information

Published: 2022/03/24, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_98.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_98.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_98.0.2+build1-0ubuntu0.20.04.1

169586 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5782-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5782-2 advisory.

USN-5782-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5782-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF

USN:5782-2

Plugin Information

Published: 2023/01/05, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_108.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_108.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_108.0.1+build1-0ubuntu0.20.04.1

169727 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5782-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5782-3 advisory.

USN-5782-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5782-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5782-3

Plugin Information

Published: 2023/01/10, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_108.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_108.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_108.0.2+build1-0ubuntu0.20.04.1

171012 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5816-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5816-2 advisory.

USN-5816-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5816-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5816-2

Plugin Information

Published: 2023/02/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_109.0.1+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_109.0.1+build1-0ubuntu0.20.04.2
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_109.0.1+build1-0ubuntu0.20.04.2

172031 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5880-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5880-2 advisory.

USN-5880-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5880-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5880-2

Plugin Information

Published: 2023/03/01, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_110.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_110.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_110.0.1+build2-0ubuntu0.20.04.1

173425 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-5954-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5954-2 advisory.

USN-5954-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5954-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5954-2

Plugin Information

Published: 2023/03/27, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_111.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_111.0.1+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_111.0.1+build2-0ubuntu0.20.04.1

174437 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-6010-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6010-2 advisory.

USN-6010-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6010-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6010-2

Plugin Information

Published: 2023/04/18, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_112.0.1+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_112.0.1+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_112.0.1+build1-0ubuntu0.20.04.1
```

174787 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-6010-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6010-3 advisory.

USN-6010-1 fixed vulnerabilities and USN-6010-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6010-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6010-3

Plugin Information

Published: 2023/04/26, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_112.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_112.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_112.0.2+build1-0ubuntu0.20.04.1

175820 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-6074-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6074-2 advisory.

USN-6074-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6074-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6074-2

Plugin Information

Published: 2023/05/16, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_113.0.1+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_113.0.1+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_113.0.1+build1-0ubuntu0.20.04.1
```

176327 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox regressions (USN-6074-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6074-3 advisory.

USN-6074-1 fixed vulnerabilities and USN-6074-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6074-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6074-3

Plugin Information

Published: 2023/05/24, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_113.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_113.0.2+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_113.0.2+build1-0ubuntu0.20.04.1
```

167273 - Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-5709-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5709-2 advisory.

USN-5709-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5709-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5709-2

Plugin Information

Published: 2022/11/10, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_106.0.5+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_106.0.5+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_106.0.5+build1-0ubuntu0.20.04.1

147988 - Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar regression (USN-4733-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4733-2 advisory.

USN-4733-1 fixed a vulnerability in GNOME Autoar. The upstream fix introduced a regression when extracting archives containing directories. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4733-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4733-2

Plugin Information

Published: 2021/03/23, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libgnome-autoar-0_0_0.2.3-2
- Fixed package : libgnome-autoar-0_0_0.2.3-2ubuntu0.2

150325 - Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar regression (USN-4937-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4937-2 advisory.

USN-4937-1 fixed a vulnerability in GNOME Autoar. The update caused a regression when extracting certain archives. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4937-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4937-2

Plugin Information

Published: 2021/06/07, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libgnome-autoar-0_0_0.2.3-2
- Fixed package : libgnome-autoar-0_0_0.2.3-2ubuntu0.4

144111 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-4658-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4658-2 advisory.

USN-4658-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression in the software raid10 driver when used with fstrim that could lead to data corruption. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4658-2>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:4658-2

Plugin Information

Published: 2020/12/13, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-58-generic for this advisory.

145512 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-4712-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4712-1 advisory.

USN-4576-1 fixed a vulnerability in the overlay file system implementation in the Linux kernel.

Unfortunately, that fix introduced a regression that could incorrectly deny access to overlay files in some situations. This update fixes the problem.

We apologize for the inconvenience.

Original vulnerability details:

Giuseppe Scrivano discovered that the overlay file system in the Linux kernel did not properly perform permission checks in some situations. A local attacker could possibly use this to bypass intended restrictions and gain read access to restricted files.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4712-1>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:4712-1

Plugin Information

Published: 2021/01/28, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-65-generic for this advisory.

156710 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-5210-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5210-2 advisory.

USN-5210-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused failures to boot in environments with AMD Secure Encrypted Virtualization (SEV) enabled. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5210-2>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:5210-2

Plugin Information

Published: 2022/01/13, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-94-generic for this advisory.

157458 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-5267-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5267-2 advisory.

USN-5267-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused the kernel to freeze when accessing CIFS shares in some situations.

This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5267-2>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:5267-2

Plugin Information

Published: 2022/02/09, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 5.4.0-42-generic does not meet the minimum fixed level of 5.4.0-99-generic for this advisory.

149405 - Ubuntu 18.04 LTS / 20.04 LTS : MariaDB vulnerabilities (USN-4944-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4944-1 advisory.

This update fixed multiple vulnerabilities in MariaDB.

Ubuntu 18.04 LTS has been updated to MariaDB 10.1.48. Ubuntu 20.04 LTS has been updated to MariaDB 10.3.29. Ubuntu 20.10 has been updated to MariaDB 10.3.29. Ubuntu 21.04 has been updated to MariaDB 10.5.10.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4944-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4944-1

Plugin Information

Published: 2021/05/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.29-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.29-0ubuntu0.20.04.1

```
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.29-0ubuntu0.20.04.1

- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.29-0ubuntu0.20.04.1

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.29-0ubuntu0.20.04.1

- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.29-0ubuntu0.20.04.1

- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.29-0ubuntu0.20.04.1
```

152954 - Ubuntu 18.04 LTS / 20.04 LTS : NTFS-3G vulnerabilities (USN-5060-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5060-1 advisory.

It was discovered that NTFS-3G incorrectly handled certain image file. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5060-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5060-1

Plugin Information

Published: 2021/09/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1
- Fixed package : libntfs-3g883_1:2017.3.23AR.3-3ubuntu1.1

- Installed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1
- Fixed package : ntfs-3g_1:2017.3.23AR.3-3ubuntu1.1
```

153593 - Ubuntu 18.04 LTS / 20.04 LTS : ca-certificates update (USN-5089-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5089-1 advisory.

The ca-certificates package contained a CA certificate that will expire on 2021-09-30 and will cause connectivity issues. This update removes the DST Root CA X3 CA.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5089-1>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5089-1

Plugin Information

Published: 2021/09/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20210119~20.04.2

161981 - Ubuntu 18.04 LTS / 20.04 LTS : ca-certificates update (USN-5473-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5473-1 advisory.

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.50 version of the Mozilla certificate authority bundle.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5473-1>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5473-1

Plugin Information

Published: 2022/06/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20211016~20.04.1

175723 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : MySQL regression (USN-6060-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6060-3 advisory.

USN-6060-1 fixed vulnerabilities in MySQL. The new upstream 8.0.33 version introduced a regression on the armhf architecture. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6060-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6060-3

Plugin Information

Published: 2023/05/15, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.33-0ubuntu0.20.04.2

201128 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Netplan regression (USN-6851-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6851-2 advisory.

USN-6851-1 fixed vulnerabilities in Netplan. The update lead to the discovery of a regression in netplan which caused systemctl enable to fail on systems where systemd is not running. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6851-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6851-2

Plugin Information

Published: 2024/06/28, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libnetplan0_0.99-0ubuntu3~20.04.2
- Fixed package : libnetplan0_0.104-0ubuntu2~20.04.6
- Installed package : netplan.io_0.99-0ubuntu3~20.04.2
- Fixed package : netplan.io_0.104-0ubuntu2~20.04.6

189775 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server regression (USN-6587-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6587-3 advisory.

USN-6587-1 fixed vulnerabilities in X.Org X Server. The fix was incomplete resulting in a possible regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6587-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6587-3

Plugin Information

Published: 2024/01/30, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-common_2:1.20.13-1ubuntu1~20.04.15
- Installed package : xserver-xephyr_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xephyr_2:1.20.13-1ubuntu1~20.04.15
- Installed package : xserver-xorg-core_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-core_2:1.20.13-1ubuntu1~20.04.15
- Installed package : xserver-xorg-legacy_2:1.20.8-2ubuntu2.2
- Fixed package : xserver-xorg-legacy_2:1.20.13-1ubuntu1~20.04.15
- Installed package : xwayland_2:1.20.8-2ubuntu2.2
- Fixed package : xwayland_2:1.20.13-1ubuntu1~20.04.15

202231 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Apache HTTP Server regression (USN-6885-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6885-2 advisory.

USN-6885-1 fixed vulnerabilities in Apache HTTP Server. One of the security fixes introduced a regression when proxying requests to a HTTP/2 server. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6885-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6885-2

Plugin Information

Published: 2024/07/11, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : apache2_2.4.41-4ubuntu3
- Fixed package : apache2_2.4.41-4ubuntu3.20

- Installed package : apache2-bin_2.4.41-4ubuntu3
- Fixed package : apache2-bin_2.4.41-4ubuntu3.20

- Installed package : apache2-data_2.4.41-4ubuntu3
- Fixed package : apache2-data_2.4.41-4ubuntu3.20

- Installed package : apache2-utils_2.4.41-4ubuntu3
- Fixed package : apache2-utils_2.4.41-4ubuntu3.20
```

171732 - Ubuntu 20.04 LTS / 22.04 LTS : MariaDB regression (USN-5739-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5739-2 advisory.

USN-5739-1 fixed vulnerabilities in MariaDB. It caused a regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5739-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5739-2

Plugin Information

Published: 2023/02/21, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.38-0ubuntu0.20.04.1
- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.38-0ubuntu0.20.04.1

160636 - Ubuntu 20.04 LTS / 22.04 LTS : MySQL regression (USN-5400-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5400-3 advisory.

USN-5400-1 fixed vulnerabilities in MySQL. The fix breaks existing charm configurations. This updated fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5400-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF

USN:5400-3

Plugin Information

Published: 2022/05/05, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.29-0ubuntu0.20.04.3

170762 - Ubuntu 20.04 LTS / 22.04 LTS : MySQL regression (USN-5823-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5823-3 advisory.

USN-5823-1 fixed vulnerabilities in MySQL. Unfortunately, 8.0.32 introduced a regression in MySQL Router preventing connections from PyMySQL. This update reverts most of the changes in MySQL Router to 8.0.31 until a proper fix can be found.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5823-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF

USN:5823-3

Plugin Information

Published: 2023/01/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.32-0ubuntu0.20.04.2

193233 - Ubuntu 20.04 LTS / 22.04 LTS : NSS regression (USN-6727-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6727-2 advisory.

USN-6727-1 fixed vulnerabilities in NSS. The update introduced a regression when trying to load security modules on Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6727-2>

Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

Risk Factor

None

References

XREF USN:6727-2

Plugin Information

Published: 2024/04/11, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libnss3_2:3.49.1-1ubuntu1.2
- Fixed package : libnss3_2:3.98-0ubuntu0.20.04.2

161481 - Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5441-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5441-1 advisory.

A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5441-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5441-1

Plugin Information

Published: 2022/05/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gir1.2-javascriptcoregtk-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-javascriptcoregtk-4.0_2.36.2-0ubuntu0.20.04.1
- Installed package : gir1.2-webkit2-4.0_2.28.3-0ubuntu0.20.04.1
- Fixed package : gir1.2-webkit2-4.0_2.36.2-0ubuntu0.20.04.1
- Installed package : libjavascriptcoregtk-4.0-18_2.28.3-0ubuntu0.20.04.1
- Fixed package : libjavascriptcoregtk-4.0-18_2.36.2-0ubuntu0.20.04.1
- Installed package : libwebkit2gtk-4.0-37_2.28.3-0ubuntu0.20.04.1
- Fixed package : libwebkit2gtk-4.0-37_2.36.2-0ubuntu0.20.04.1

207769 - Ubuntu 20.04 LTS / 22.04 LTS : ca-certificates update (USN-7034-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7034-1 advisory.

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.64 version of the Mozilla certificate authority bundle.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-7034-1>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:7034-1

Plugin Information

Published: 2024/09/25, Modified: 2024/09/25

Plugin Output

tcp/0

- Installed package : ca-certificates_20190110ubuntu1.1
- Fixed package : ca-certificates_20240203~20.04.1

177216 - Ubuntu 20.04 LTS : Firefox regressions (USN-6143-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6143-2 advisory.

USN-6143-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6143-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6143-2

Plugin Information

Published: 2023/06/13, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_114.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_114.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_114.0.1+build1-0ubuntu0.20.04.1

177463 - Ubuntu 20.04 LTS : Firefox regressions (USN-6143-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6143-3 advisory.

USN-6143-1 fixed vulnerabilities and USN-6143-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6143-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6143-3

Plugin Information

Published: 2023/06/21, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_114.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_114.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_114.0.2+build1-0ubuntu0.20.04.1

179436 - Ubuntu 20.04 LTS : Firefox regressions (USN-6267-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6267-2 advisory.

USN-6267-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6267-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6267-2

Plugin Information

Published: 2023/08/08, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_116.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_116.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_116.0.2+build1-0ubuntu0.20.04.1

180003 - Ubuntu 20.04 LTS : Firefox regressions (USN-6267-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6267-3 advisory.

USN-6267-1 fixed vulnerabilities and USN-6267-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6267-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6267-3

Plugin Information

Published: 2023/08/21, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_116.0.3+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_116.0.3+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_116.0.3+build2-0ubuntu0.20.04.1

182892 - Ubuntu 20.04 LTS : Firefox regressions (USN-6404-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6404-2 advisory.

USN-6404-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6404-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6404-2

Plugin Information

Published: 2023/10/11, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_118.0.2+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_118.0.2+build2-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_118.0.2+build2-0ubuntu0.20.04.1

185512 - Ubuntu 20.04 LTS : Firefox regressions (USN-6456-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6456-2 advisory.

USN-6456-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6456-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6456-2

Plugin Information

Published: 2023/11/14, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_119.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_119.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_119.0.1+build1-0ubuntu0.20.04.1

186534 - Ubuntu 20.04 LTS : Firefox regressions (USN-6509-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6509-2 advisory.

USN-6509-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6509-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6509-2

Plugin Information

Published: 2023/12/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_120.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_120.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_120.0.1+build1-0ubuntu0.20.04.1

187938 - Ubuntu 20.04 LTS : Firefox regressions (USN-6562-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6562-2 advisory.

USN-6562-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6562-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6562-2

Plugin Information

Published: 2024/01/11, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_121.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_121.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_121.0.1+build1-0ubuntu0.20.04.1

190093 - Ubuntu 20.04 LTS : Firefox regressions (USN-6610-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6610-2 advisory.

USN-6610-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6610-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6610-2

Plugin Information

Published: 2024/02/07, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_122.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_122.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_122.0.1+build1-0ubuntu0.20.04.1

191630 - Ubuntu 20.04 LTS : Firefox regressions (USN-6649-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6649-2 advisory.

USN-6649-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6649-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6649-2

Plugin Information

Published: 2024/03/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_123.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_123.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_123.0.1+build1-0ubuntu0.20.04.1

192918 - Ubuntu 20.04 LTS : Firefox regressions (USN-6710-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6710-2 advisory.

USN-6710-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6710-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6710-2

Plugin Information

Published: 2024/04/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_124.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_124.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_124.0.2+build1-0ubuntu0.20.04.1

194903 - Ubuntu 20.04 LTS : Firefox regressions (USN-6747-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6747-2 advisory.

USN-6747-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6747-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6747-2

Plugin Information

Published: 2024/05/02, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_125.0.3+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_125.0.3+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_125.0.3+build1-0ubuntu0.20.04.1

198064 - Ubuntu 20.04 LTS : Firefox regressions (USN-6779-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6779-2 advisory.

USN-6779-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6779-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6779-2

Plugin Information

Published: 2024/05/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_126.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_126.0.1+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_126.0.1+build1-0ubuntu0.20.04.1

206006 - Ubuntu 20.04 LTS : Firefox regressions (USN-6966-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6966-2 advisory.

USN-6966-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6966-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6966-2

Plugin Information

Published: 2024/08/21, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_129.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_129.0.2+build1-0ubuntu0.20.04.1
- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_129.0.2+build1-0ubuntu0.20.04.1

207582 - Ubuntu 20.04 LTS : Firefox regressions (USN-6992-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6992-2 advisory.

USN-6992-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6992-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6992-2

Plugin Information

Published: 2024/09/23, Modified: 2024/09/23

Plugin Output

tcp/0

- Installed package : firefox_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox_130.0.1+build1-0ubuntu0.20.04.1

```
- Installed package : firefox-locale-de_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-de_130.0.1+build1-0ubuntu0.20.04.1

- Installed package : firefox-locale-en_78.0.2+build2-0ubuntu0.20.04.1
- Fixed package : firefox-locale-en_130.0.1+build1-0ubuntu0.20.04.1
```

152134 - Ubuntu 20.04 LTS : MariaDB regression (USN-4944-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4944-2 advisory.

USN-4944-1 fixed vulnerabilities in MariaDB. It caused a regression. This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4944-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4944-2

Plugin Information

Published: 2021/07/28, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : mariadb-client_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-client-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-10.3_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-client-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-client-core-10.3_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-common_1:10.3.22-1ubuntu1
- Fixed package : mariadb-common_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-server_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-server-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-10.3_1:10.3.30-0ubuntu0.20.04.1

- Installed package : mariadb-server-core-10.3_1:10.3.22-1ubuntu1
- Fixed package : mariadb-server-core-10.3_1:10.3.30-0ubuntu0.20.04.1
```

143374 - Ubuntu 20.04 LTS : MySQL vulnerabilities (USN-4651-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4651-1 advisory.

Tom Reynolds discovered that due to a packaging error, the MySQL X Plugin was listening to all network interfaces by default, contrary to expectations.

This update changes the default MySQL configuration to bind the MySQL X Plugin to localhost only. This change may impact environments where the MySQL X Plugin needs to be accessible from the network. The mysqlx-bind-address setting in the /etc/mysql/mysql.conf.d/mysqld.cnf file can be modified to allow network access.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-4651-1>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4651-1

Plugin Information

Published: 2020/12/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient21_8.0.21-0ubuntu0.20.04.3
- Fixed package : libmysqlclient21_8.0.22-0ubuntu0.20.04.3

156041 - Ubuntu 20.04 LTS : Samba regression (USN-5142-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5142-3 advisory.

USN-5142-1 fixed vulnerabilities in Samba. Some of the upstream changes introduced a regression in Kerberos authentication in certain environments.

Please see the following upstream bug for more information:

https://bugzilla.samba.org/show_bug.cgi?id=14922

This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5142-3>

Solution

Update the affected packages.

Risk Factor

None

References

XREF

USN:5142-3

Plugin Information

Published: 2021/12/13, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : lib smbclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : lib smbclient_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : lib wbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : lib wbclient0_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.14+dfsg-0ubuntu0.20.04.4

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.14+dfsg-0ubuntu0.20.04.4
```

170727 - Ubuntu 20.04 LTS : Samba regression (USN-5822-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5822-2 advisory.

USN-5822-1 fixed vulnerabilities in Samba. The update for Ubuntu 20.04 LTS introduced regressions in certain environments. Pending investigation of these regressions, this update temporarily reverts the security fixes.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5822-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5822-2

Plugin Information

Published: 2023/01/27, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.17~dfsg-0ubuntu1.20.04.5

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.17~dfsg-0ubuntu1.20.04.5
```

182944 - Ubuntu 20.04 LTS : Samba regression (USN-6425-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6425-2 advisory.

USN-6425-1 fixed vulnerabilities in Samba. Due to a build issue on Ubuntu 20.04 LTS, the update introduced regressions in macro handling and possibly other functionality.

This update fixes the problem. We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-6425-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6425-2

Plugin Information

Published: 2023/10/11, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libsmclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libsmclient_2:4.15.13+dfsg-0ubuntu0.20.04.7

- Installed package : libwbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : libwbclient0_2:4.15.13+dfsg-0ubuntu0.20.04.7

- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.15.13+dfsg-0ubuntu0.20.04.7
```

- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.15.13+dfsg-0ubuntu0.20.04.7
- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.15.13+dfsg-0ubuntu0.20.04.7
- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.15.13+dfsg-0ubuntu0.20.04.7
- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.15.13+dfsg-0ubuntu0.20.04.7
- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.15.13+dfsg-0ubuntu0.20.04.7
- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.15.13+dfsg-0ubuntu0.20.04.7

155892 - Ubuntu 20.04 LTS : Samba regressions (USN-5142-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5142-2 advisory.

USN-5142-1 fixed vulnerabilities in Samba. Some of the upstream changes introduced regressions in name mapping and backups.

Please see the following upstream bugs for more information:

https://bugzilla.samba.org/show_bug.cgi?id=14901 https://bugzilla.samba.org/show_bug.cgi?id=14918

This update fixes the problem.

Tenable has extracted the preceding description block directly from the Ubuntu 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://ubuntu.com/security/notices/USN-5142-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5142-2

Plugin Information

Published: 2021/12/07, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : lib smbclient_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : lib smbclient_2:4.13.14+dfsg-0ubuntu0.20.04.3
- Installed package : lib wbclient0_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : lib wbclient0_2:4.13.14+dfsg-0ubuntu0.20.04.3
- Installed package : python3-samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : python3-samba_2:4.13.14+dfsg-0ubuntu0.20.04.3
- Installed package : samba_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba_2:4.13.14+dfsg-0ubuntu0.20.04.3
- Installed package : samba-common_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common_2:4.13.14+dfsg-0ubuntu0.20.04.3
- Installed package : samba-common-bin_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-common-bin_2:4.13.14+dfsg-0ubuntu0.20.04.3

```
- Installed package : samba-dsdb-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-dsdb-modules_2:4.13.14+dfsg-0ubuntu0.20.04.3

- Installed package : samba-libs_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-libs_2:4.13.14+dfsg-0ubuntu0.20.04.3

- Installed package : samba-vfs-modules_2:4.11.6+dfsg-0ubuntu1.3
- Fixed package : samba-vfs-modules_2:4.13.14+dfsg-0ubuntu0.20.04.3
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.3 0.2 167960 11700 ? Ss 01:13 0:06 /sbin/init auto noprompt
root 2 0.0 0.0 0 0 ? S 01:13 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? I< 01:13 0:00 [rcu_gp]
root 4 0.0 0.0 0 0 ? I< 01:13 0:00 [rcu_par_gp]
root 6 0.0 0.0 0 0 ? I< 01:13 0:00 [kworker/0:0H-kblockd]
root 7 0.0 0.0 0 0 ? I 01:13 0:01 [kworker/0:1-memcg_kmem_cache]
root 9 0.0 0.0 0 0 ? I< 01:13 0:00 [mm_percpu_wq]
root 10 0.0 0.0 0 0 ? S 01:13 0:00 [ksoftirqd/0]
root 11 0.1 0.0 0 0 ? I 01:13 0:02 [rcu_sched]
root 12 0.0 0.0 0 0 ? S 01:13 0:00 [migration/0]
root 13 0.0 0.0 0 0 ? S 01:13 0:00 [idle_inject/0]
root 14 0.0 0.0 0 0 ? S 01:13 0:00 [cpuhp/0]
root 15 0.0 0.0 0 0 ? S 01:13 0:00 [cpuhp/1]
root 16 0.0 0.0 0 0 ? S 01:13 0:00 [idle_inject/1]
root 17 0.0 0.0 0 0 ? S 01:13 0:01 [migration/1]
root 18 0.0 0.0 0 0 ? S 01:13 0:00 [ksoftirqd/1]
root 19 0.0 0.0 0 0 ? I 01:13 0:00 [kworker/1:0-events]
root 20 0.0 0.0 0 0 ? I< 01:13 0:00 [kworker/1:0H-kblockd]
root 21 0.0 0.0 0 0 ? S 01:13 0:00 [cpuhp/2]
root 22 0.0 0.0 0 0 ? S 01:13 0:00 [idle_inject/2]
root 23 0.0 0.0 0 0 ? S 01:13 0:01 [migration/2]
root 24 0.0 0.0 0 0 ? S 01:13 0:00 [ksoftirqd/2]
root 26 0.0 0.0 0 0 ? I< 01:13 0:00 [kworker/2:0H-kblockd]
root 27 0.0 0.0 0 0 ? S 01:13 0:00 [cpuhp/3]
root 28 0.0 0.0 0 0 ? S 01:13 0:00 [idle_inject/3]
root 29 0.0 0.0 0 0 ? S 01:13 0:01 [migration/3]
root 30 0.2 0.0 0 0 ? S 01:13 0:04 [ksoftirqd/3]
root 32 0.0 0.0 0 0 ? I< 01:13 0:00 [kworker/3:0H-kblockd]
root 33 0.0 0.0 0 0 ? S 01:13 0:00 [kdevtmpfs]
root 34 0.0 0.0 0 0 ? I< 01:13 0:00 [netns]
root 35 0.0 0.0 0 0 ? S 01:13 0:00 [rcu_tasks_kthre]
root 36 0.0 0.0 0 0 ? S 01:13 0:00 [kauditfd]
root 37 0.0 0.0 0 0 ? S 01:13 0:00 [khungtaskd]
root 38 0.0 0.0 0 0 ? S 01:13 0:00 [oom_reaper]
root 39 0.0 0.0 0 0 ? I< 01:13 0:00 [writeback]
root 40 0.0 0.0 0 0 ? S 01:13 0:00 [kcompactd0]
root 41 0.0 0.0 0 0 ? SN 01:13 0:00 [ksmd]
root 42 0.0 0.0 0 0 ? SN 01:13 0:00 [khugepaged]
root 47 0.0 0.0 0 0 ? I 01:13 0:00 [kworker/3:1-cgroup_destroy]
root 135 0.0 0.0 0 0 ? I< 01:13 0:00 [kintegrityd]
root 136 0.0 0.0 0 0 ? I< 01:13 0:00 [kblockd]
root 137 0.0 0.0 0 0 ? I< 01:13 0:00 [blkcg_punt_bio]
root 138 0.0 0.0 0 0 ? I< 01:13 0:00 [tpm_dev_wq]
root 139 0.0 0.0 0 0 ? I< 01:13 0:00 [ata_sff]
root 140 0.0 0.0 0 0 ? I< 01:13 0:00 [md]
root 141 0.0 0.0 0 0 ? I< 01:13 0:00 [edac-poller]
root 142 0.0 0.0 0 0 ? I< 01:13 0:00 [devfreq_wq]
root 143 0.0 0.0 0 0 ? S 01:13 0:00 [watchdogd]
root 149 0.0 0.0 0 0 ? S 01:13 0:00 [kswapd0]
root 150 0.0 0.0 0 0 ? S 01:13 0:00 [ecryptfs-kthrea]
root 153 0.0 0.0 0 0 ? I< 01:13 0:00 [kthrotld]
```

```

root 154 0.0.0.0 0 0 ? I< 01:13 0:00 [acpi_thermal_pm]
root 155 0.0.0.0 0 0 ? I< 01:13 0:00 [vfio-irqfd-clea]
root 156 0.0.0.0 0 0 ? I< 01:13 0:00 [ipv6_addrconf]
root 167 0.0.0.0 0 0 ? I< 01:13 0:00 [kstrp]
root 171 0.0.0.0 0 0 ? I< 01:13 0:00 [kworker/u9:0]
root 187 0.0.0.0 0 0 ? I< 01:13 0:00 [charger_manager]
root 233 0.0.0.0 0 0 ? I< 01:13 0:00 [mpt_poll_0]
root 234 0.0.0.0 0 0 ? I< 01:13 0:00 [mpt/0]
root 235 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_0]
root 236 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_0]
root 237 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_1]
root 238 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_1]
root 239 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_2]
root 240 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_2]
root 241 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_3]
root 242 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_3]
root 243 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_4]
root 244 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_4]
root 245 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_5]
root 246 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_5]
root 247 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_6]
root 248 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_6]
root 249 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_7]
root 250 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_7]
root 251 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_8]
root 252 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_8]
root 253 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_9]
root 254 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_9]
root 255 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_10]
root 256 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_10]
root 257 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_11]
root 258 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_11]
root 259 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_12]
root 260 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_12]
root 261 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_13]
root 262 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_13]
root 263 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_14]
root 264 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_14]
root 265 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_15]
root 266 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_15]
root 267 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_16]
root 268 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_16]
root 269 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_17]
root 270 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_17]
root 271 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_18]
root 272 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_18]
root 273 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_19]
root 274 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_19]
root 275 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_20]
root 276 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_20]
root 277 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_21]
root 278 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_21]
root 279 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_22]
root 280 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_22]
root 281 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_23]
root 282 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_23]
root 283 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_24]
root 284 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_24]
root 285 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_25]
root 286 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_25]
root 287 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_26]
root 288 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_26]
root 289 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_27]
root 290 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_27]
root 291 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_28]
root 292 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_28]
root 293 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_29]
root 294 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_29]
root 321 0.0.0.0 0 0 ? I 01:13 0:00 [kworker/u8:28-events_unbound]
root 324 0.0.0.0 0 0 ? S 01:13 0:00 [scsi_eh_30]
root 325 0.0.0.0 0 0 ? I< 01:13 0:00 [scsi_tmf_30]
root 326 0.0.0.0 0 0 ? I< 01:13 0:00 [kworker/2:1H-kblockd]
root 352 0.0.0.0 0 0 ? I< 01:14 0:00 [kworker/1:1H-kblockd]
root 354 0.0.0.0 0 0 ? I< 01:14 0:00 [kworker/0:1H-kblockd]
root 355 0.0.0.0 0 0 ? S 01:14 0:00 [jbd2/sda5-8]
root 356 0.0.0.0 0 0 ? I< 01:14 0:00 [ext4-rsv-conver]
root 368 0.0.0.0 0 0 ? I 01:14 0:00 [kworker/3:1H-kblockd]
root 397 0.0.0.5 69884 22064 ? S< 01:14 0:01 /lib/systemd/systemd-journald
root 428 0.1 0.1 23708 7048 ? Ss 01:14 0:02 /lib/systemd/systemd-udev
root 431 0.0.0.0 0 0 ? S< 01:14 0:00 [loop0]
root 439 0.0.0.0 0 0 ? S< 01:14 0:00 [loop1]
root 443 0.0.0.0 0 0 ? S< 01:14 0:00 [loop2]
root 446 0.0.0.0 0 0 ? S< 01:14 0:00 [loop3]
root 449 0.0.0.0 0 0 ? S< 01:14 0:00 [loop4]
root 450 0.0.0.0 0 0 ? S< 01:14 0:00 [loop5]
root 451 0.0.0.0 0 0 ? S< 01:14 0:00 [loop6]
root 452 0.0.0.0 0 0 ? S< 01:14 0:00 [loop7]
root 454 0.0.0.0 0 0 ? S< 01:14 0:00 [loop8]
root 455 0.0.0.0 0 0 ? S< 01:14 0:00 [loop9]
root 464 0.0.0.0 0 0 ? S< 01:14 0:00 [loop10]
root 481 0.0.0.0 0 0 ? I< 01:14 0:00 [ttm_swap]
root 482 0.0.0.0 0 0 ? I< 01:14 0:00 [iprt-VBoxWQueue]
root 490 0.0.0.0 0 0 ? I< 01:14 0:00 [cryptd]
systemd+ 660 0.0.0.3 24056 12104 ? Ss 01:14 0:00 /lib/systemd/systemd-resolved
systemd+ 663 0.0.0.1 90424 6352 ? Ssl 01:14 0:00 /lib/systemd/systemd-timesyncd
root 681 0.0.0.1 247180 7792 ? Ssl 01:14 0:00 /usr/lib/accountsservice/accounts-daemon
root 682 0.0.0.0 2540 724 ? Ss 01:14 0:00 /usr/sbin/acpid
avahi 684 0.0.0.0 8500 3512 ? Ss 01:14 0:00 avahi-daemon: running [ubuntu.local]
root 685 0.0.0.0 18060 3196 ? Ss 01:14 0:00 /usr/sbin/cron -f

```

```

root 686 0.0.2 36812 8472 ? Ss 01:14 0:00 /usr/sbin/cupsd -l
message+ 688 0.2 0.1 8876 5868 ? Rs 01:14 0:05 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root 689 0.1 0.5 271244 20264 ? Ssl 01:14 0:03 /usr/sbin/NetworkManager --no-daemon
root 697 0.0 0.0 81808 3704 ? Ssl 01:14 0:00 /usr/sbin/irqbalance --foreground
root 699 0.0 0.5 47904 20252 ? Ss 01:14 0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
root 705 0.4 0.2 234916 9928 ? Ssl 01:14 0:08 /usr/lib/policykit-1/polkitd --no-debug
syslog 710 0.0 0.1 224324 4432 ? Ssl 01:14 0:00 /usr/sbin/rsyslogd -n -iNONE
root 714 0.3 0.8 1146576 33920 ? Ssl 01:14 0:07 /usr/lib/snapd/snapd
root 719 0.0 0.1 244368 6328 ? Ssl 01:14 0:00 /usr/libexec/switcheroo-control
root 724 0.0 0.2 17100 8460 ? Ss 01:14 0:01 /lib/systemd/systemd-logind
root 730 0.0 0.3 392788 12296 ? Ssl 01:14 0:00 /usr/lib/udisks2/udisksd
root 733 0.0 0.1 13664 4860 ? Ss 01:14 0:00 /sbin/wpa_supplicant -u -s -0 /run/wpa_supplicant
avahi 742 0.0 0.0 8320 332 ? S 01:14 0:00 avahi-daemon: chroot helper
root 773 0.0 0.3 180432 12776 ? Ssl 01:14 0:00 /usr/sbin/cups-browsed
lp 774 0.0 0.1 15320 6556 ? S 01:14 0:00 /usr/lib/cups/notifier/dbus dbus://
root 776 0.0 0.2 313728 10340 ? Ssl 01:14 0:00 /usr/sbin/ModemManager --filter-policy=strict
root 795 0.0 0.5 126688 22496 ? Ssl 01:14 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root 816 0.0 0.1 12168 7344 ? Ss 01:14 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root 817 0.0 0.0 0 0 ? I 01:14 0:02 [kworker/0:4-memcg_kmem_cache]
root 824 0.0 0.2 248272 8628 ? Ssl 01:14 0:00 /usr/sbin/gdm3
root 837 0.0 0.2 175424 9292 ? Sl 01:14 0:00 gdm-session-worker [pam/gdm-launch-environment]
mysql 885 0.7 2.9 1860956 120604 ? Ssl 01:14 0:15 /usr/sbin/mysqld
root 910 0.0 0.7 228588 30848 ? Ss 01:14 0:01 /usr/sbin/apache2 -k start
www-data 929 0.0 0.9 246324 40280 ? S 01:14 0:00 /usr/sbin/apache2 -k start
root 938 0.0 0.3 45188 13608 ? Ss 01:14 0:00 /usr/sbin/nmbd --foreground --no-process-group
whoopsie 940 0.0 0.3 326856 15688 ? Ssl 01:14 0:00 /usr/bin/whoopsie -f
gdm 941 0.0 0.2 19148 10384 ? Ss 01:14 0:01 /lib/systemd/systemd --user
kernooops 944 0.0 0.0 11244 448 ? Ss 01:14 0:00 /usr/sbin/kerneloops --test
kernooops 946 0.0 0.0 11244 448 ? Ss 01:14 0:00 /usr/sbin/kerneloops
gdm 948 0.0 0.0 169224 3560 ? S 01:14 0:00 (sd-pam)
gdm 970 0.0 0.3 1075772 14664 ? S<sl 01:14 0:00 /usr/bin/pulseaudio --daemonize=no --log-target=journal
gdm 972 0.0 0.6 520368 24660 ? Sns1 01:14 0:00 /usr/libexec/tracker-miner-fs
gdm 974 0.0 0.1 170452 5896 ttty1 Ssl+ 01:14 0:00 /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart
/usr/share/gdm/greeter/autostart
gdm 976 0.0 0.1 7792 5032 ? Ss 01:14 0:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root 1011 0.0 0.5 60192 22964 ? Ss 01:14 0:00 /usr/sbin/smbd --foreground --no-process-group
rtkit 1012 0.0 0.0 152916 3004 ? Sns1 01:14 0:00 /usr/libexec/rtkit-daemon
gdm 1025 0.0 0.3 271372 14656 ttty1 Sl+ 01:14 0:00 /usr/libexec/gnome-session-binary --systemd --autostart
/usr/share/gdm/greeter/autostart
gdm 1032 0.0 0.1 248544 8052 ? Ssl 01:14 0:00 /usr/libexec/gvfsd
gdm 1065 0.0 0.1 312804 6368 ? Sl 01:14 0:00 /usr/libexec/gvfsd-fuse /run/user/125/gvfs -f -o big_writes
gdm 1067 0.0 0.2 322888 9416 ? Ssl 01:14 0:00 /usr/libexec/gvfs-udisks2-volume-monitor
root 1078 0.0 0.1 57976 7260 ? S 01:14 0:00 /usr/sbin/smbd --foreground --no-process-group
root 1080 0.0 0.1 57984 5596 ? S 01:14 0:00 /usr/sbin/smbd --foreground --no-process-group
gdm 1085 0.0 0.2 325564 9056 ? Ssl 01:14 0:00 /usr/libexec/gvfs-afc-volume-monitor
root 1092 0.0 0.2 60184 9752 ? S 01:14 0:00 /usr/sbin/smbd --foreground --no-process-group
gdm 1102 0.0 0.1 98864 4396 ? Ssl 01:14 0:00 /usr/libexec/gnome-session-ctl --monitor
gdm 1104 0.0 0.1 244472 5696 ? Ssl 01:14 0:00 /usr/libexec/gvfs-ntp-volume-monitor
gdm 1114 0.0 0.1 248984 6232 ? Sl 01:14 0:00 /usr/bin/gnome-keyring-daemon --start --components ssh
gdm 1119 0.0 0.1 246748 6328 ? Ssl 01:14 0:00 /usr/libexec/gvfs-gphoto2-volume-monitor
gdm 1127 0.0 0.3 493116 15744 ? Ssl 01:14 0:00 /usr/libexec/gnome-session-binary --systemd-service --session=gnome-login
gdm 1130 0.0 0.1 244708 6444 ? Ssl 01:14 0:00 /usr/libexec/gvfs-goa-volume-monitor
gdm 1136 0.0 0.8 550508 36072 ? Sl 01:14 0:00 /usr/libexec/goa-daemon
gdm 1146 0.5 4.7 4617808 191832 ? Ssl 01:14 0:11 /usr/bin/gnome-shell
gdm 1182 0.0 0.2 323584 9228 ? Sl 01:14 0:00 /usr/libexec/goa-identity-service
root 1196 0.0 0.2 252748 9776 ? Ssl 01:14 0:00 /usr/lib/upower/upowerd
gdm 1286 0.0 0.1 305376 6372 ? Ssl 01:14 0:00 /usr/libexec/at-spi-bus-launcher
gdm 1292 0.0 0.0 7224 3932 ? S 01:14 0:00 /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
gdm 1308 0.0 1.0 715076 40344 ? Sl 01:14 0:00 /usr/bin/Xwayland :1024 -rootless -noreset -accessx -core -auth /run/user/125/.mutter-Xwaylandauth.R228E3 -listen 4 -listen 5 -displayfd 6 -listen 7
gdm 1324 0.0 0.1 244536 6120 ? Ssl 01:14 0:00 /usr/libexec/xdg-permission-store
gdm 1339 0.0 0.1 162752 6948 ? Ssl 01:14 0:00 /usr/libexec/at-spi2-registryd --use-gnome-session
gdm 1340 0.0 0.6 2724544 27052 ? Sl 01:14 0:00 /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
gdm 1346 0.0 0.1 318672 6936 ? Ssl 01:14 0:00 /usr/libexec/gsd-a11y-settings
gdm 1352 0.0 0.6 434864 25344 ? Ssl 01:14 0:00 /usr/libexec/gsd-color
gdm 1354 0.0 0.5 349680 23324 ? Ssl 01:14 0:00 /usr/libexec/gsd-keyboard
gdm 1356 0.0 0.6 618092 25412 ? Ssl 01:14 0:00 /usr/libexec/gsd-media-keys
gdm 1358 0.0 0.5 350224 23676 ? Ssl 01:14 0:00 /usr/libexec/gsd-power
gdm 1362 0.0 0.2 256956 11376 ? Ssl 01:14 0:00 /usr/libexec/gsd-print-notifications
gdm 1366 0.0 0.1 465956 6424 ? Ssl 01:14 0:00 /usr/libexec/gsd-rfkill
gdm 1368 0.0 0.2 324040 10384 ? Ssl 01:14 0:00 /usr/libexec/gsd-smartcard
gdm 1373 0.0 0.2 328260 9440 ? Ssl 01:14 0:00 /usr/libexec/gsd-sound
gdm 1380 0.0 0.1 393972 7676 ? Ssl 01:14 0:00 /usr/libexec/gsd-usb-protection
gdm 1388 0.0 0.5 423068 22892 ? Ssl 01:14 0:00 /usr/libexec/gsd-wacom
gdm 1392 0.0 0.2 322992 8516 ? Ssl 01:14 0:00 /usr/libexec/gsd-wwan
gdm 1410 0.0 0.3 351044 15476 ? Sl 01:14 0:00 /usr/libexec/gsd-printer
colord 1457 0.0 0.3 255128 14836 ? Ssl 01:14 0:00 /usr/libexec/colord
gdm 1467 0.0 0.2 393620 8672 ? Sl 01:14 0:00 ibus-daemon --panel disable -r --xim
gdm 1469 0.0 1.4 1050164 60048 ? Ssl 01:14 0:00 /usr/libexec/gsd-xsettings
gdm 1474 0.0 0.1 171620 7316 ? Sl 01:14 0:00 /usr/libexec/ibus-memconf
gdm 1477 0.0 1.4 901444 58636 ? Ssl 01:14 0:00 /usr/libexec/ibus-x11 --kill-daemon
gdm 1481 0.0 0.1 245416 7364 ? Sl 01:14 0:00 /usr/libexec/ibus-portal
gdm 1488 0.0 0.1 171612 7368 ? Sl 01:14 0:00 /usr/libexec/ibus-engine-simple
root 1622 0.0 0.0 0 ? I 01:25 0:00 [kworker/1:1-events]
gdm 1804 0.0 1.7 501768 69916 ? Ssl 01:25 0:01 /usr/bin/python3 /usr/lib/ubuntu-release-upgrader/check-new-release-gtk
root 1843 0.0 0.0 0 ? I 01:29 0:00 [kworker/2:0-cgroup_destroy]
root 1847 0.0 0.0 0 ? I 01:29 0:00 [kworker/2:3-events]
root 1864 0.0 0.0 0 ? I 01:29 0:00 [kworker/3:0-events]
www-data 1892 0.0 0.3 229112 14824 ? S 01:36 0:00 /usr/sbin/apache2 -k start
www-data 1913 0.0 0.3 229112 14828 ? S 01:36 0:00 /usr/sbin/apache2 -k start
root 1933 0.0 0.0 0 ? I 01:36 0:00 [kworker/u8:1-events_power_efficient]
www-data 1957 0.0 0.3 229112 14744 ? S 01:37 0:00 /usr/sbin/apache2 -k start
www-data 1959 0.0 0.3 229120 14832 ? S 01:37 0:00 /usr/sbin/apache2 -k start
www-data 1965 0.0 0.3 229112 14828 ? S 01:37 0:00 /usr/sbin/apache2 -k start
www-data 1966 0.0 0.3 229112 14824 ? S 01:37 0:00 /usr/sbin/apache2 -k start

```

```

www-data 1968 0.0 0.3 229112 14824 ? S 01:37 0:00 /usr/sbin/apache2 -k start
www-data 1997 0.0 0.3 229112 14824 ? S 01:37 0:00 /usr/sbin/apache2 -k start
www-data 1999 0.0 0.3 229112 14824 ? S 01:37 0:00 /usr/sbin/apache2 -k start
root 2044 0.0 0.0 0.0 ? I 01:45 0:00 [kworker/0:0-events]
root 2193 0.0 0.0 0.0 ? I 01:46 0:00 [kworker/3:2-events]
root 2203 0.1 0.0 0.0 ? R 01:46 0:00 [kworker/2:1-events]
root 2446 0.0 0.0 0.0 ? I 01:46 0:00 [kworker/u8:0-events_unbound]
root 2495 0.0 0.0 0.0 ? I 01:46 0:00 [kworker/2:2-events]
root 2977 0.0 0.0 0.0 ? I 01:47 0:00 [kworker/1:2-events]
root 3000 0.0 0.0 0.0 ? I 01:47 0:00 [kworker/u8:2-events_unbound]
root 3648 0.0 0.0 0.0 ? I 01:48 0:00 [kworker/0:2]
root 3658 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3659 0.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3660 0.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3661 0.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3662 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3663 3.7 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3664 1.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3665 0.5 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3666 0.5 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3667 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3668 4.5 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3669 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3670 2.5 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3671 3.4 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
silky 3672 1.4 0.2 18780 9856 ? Ss 01:48 0:00 /lib/systemd/systemd --user
silky 3673 0.0 0.0 169352 3640 ? S 01:48 0:00 (sd-pam)
silky 3680 1.6 0.8 1216796 35340 ? Sns1 01:48 0:00 /usr/libexec/tracker-extract
silky 3681 2.1 0.6 594108 24848 ? Sns1 01:48 0:00 /usr/libexec/tracker-miner-fs
silky 3684 0.6 0.1 7372 4472 ? Ss 01:48 0:00 /usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
silky 3699 0.0 0.1 248544 7784 ? Ssl 01:48 0:00 /usr/libexec/gvfsd
silky 3706 0.0 0.1 312804 6444 ? S1 01:48 0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f -o big_writes
silky 3723 0.3 0.2 322760 9032 ? Ssl 01:48 0:00 /usr/libexec/gvfs-udisks2-volume-monitor
silky 3788 0.0 0.2 325564 8692 ? Ssl 01:48 0:00 /usr/libexec/gvfs-afc-volume-monitor
silky 3814 0.0 0.1 244472 5316 ? Ssl 01:48 0:00 /usr/libexec/gvfs-mtp-volume-monitor
silky 3823 0.0 0.1 246748 6100 ? Ssl 01:48 0:00 /usr/libexec/gvfs-gphoto2-volume-monitor
silky 3827 0.1 0.1 244708 6048 ? Ssl 01:48 0:00 /usr/libexec/gvfs-goa-volume-monitor
silky 3839 1.1 0.8 624368 35848 ? Sl 01:48 0:00 /usr/libexec/goa-daemon
silky 3875 0.0 0.2 323716 8616 ? Sl 01:48 0:00 /usr/libexec/goa-identity-service
silky 3992 1.3 0.5 370016 22436 ? Ssl 01:48 0:00 /usr/libexec/tracker-store
root 3993 0.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3994 1.8 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3995 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3996 0.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3997 4.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 3998 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 4000 3.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 4007 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 4008 0.0 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 4009 1.1 0.1 23708 4912 ? S 01:48 0:00 /lib/systemd/systemd-udevd
root 5831 1.0 0.2 13988 8864 ? Ss 01:48 0:00 sshd: silky [priv]
root 5918 2.0 0.2 13988 9044 ? Ss 01:48 0:00 sshd: silky [priv]
root 6164 0.0 0.2 13988 8832 ? Ss 01:48 0:00 sshd: silky [priv]
silky 6165 0.0 0.1 13988 6320 ? S 01:48 0:00 sshd: silky@notty
root 6178 0.0 0.0 0.0 ? I 01:48 0:00 [kworker/3:3-events]
silky 6193 0.0 0.1 13988 6288 ? S 01:48 0:00 sshd: silky@notty
silky 6195 0.0 0.0 18132 3172 ? Ss 01:48 0:00 bash -c /bin/ps auxww 2>/dev/null
silky 6196 0.0 0.0 20192 3396 ? R 01:48 0:00 /bin/ps auxww

```

152742 - Unix Software Discovery Commands Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

Unix software discovery checks are available.

Account : silky
Protocol : SSH

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

<https://kb.vmware.com/s/article/340>
<http://www.nessus.org/u?c0628155>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/07/28

Plugin Output

tcp/0

Path : /usr/bin/vmtoolsd
Version : 11.1.0

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

<https://www.vim.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/07/28

Plugin Output

tcp/0

Path : /usr/bin/vim.tiny
Version : 8.1

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vulnerabilities that exist on the remote host.

See Also

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2025/07/21

Plugin Output

tcp/445/cifs

Can't connect to the 'root\CIMV2' WMI namespace.

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

<http://www.robotstxt.org/orig.html>

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

Contents of robots.txt :

```
User-Agent: *
Disallow:
Disallow: /tiki/
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

The following 7 NetBIOS names have been gathered :

UBUNTU = Computer name
UBUNTU = Messenger Service
UBUNTU = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Workgroup / Domain name
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.

198234 - gnome-shell Installed (Linux / UNIX)

Synopsis

gnome-shell is installed on the remote Linux / UNIX host.

Description

gnome-shell is installed on the remote Linux / UNIX host.

See Also

<https://gitlab.gnome.org/GNOME/gnome-shell/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of GNOME Shell:

Path : /usr/bin/gnome-shell
Version : 3.36.3
Managed : 1

Path : /bin/gnome-shell
Version : 3.36.3
Managed : 1

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

curl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of curl:

```
Path : libcurl4 7.68.0-1ubuntu2.1 (via package manager)
Version : 7.68.0
Managed by OS : True

Path : libcurl3-gnutls 7.68.0-1ubuntu2.1 (via package manager)
Version : 7.68.0
Managed by OS : True
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://exiv2.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/07/28

Plugin Output

tcp/0

Path : libexiv2-27 0.27.2-8ubuntu2 (via package manager)
Version : 0.27.2
Managed by OS : True

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname : ubuntu.local.
- Advertised services :
 - o Service name : UBUNTU._smb._tcp.local.
Port number : 445
 - o Service name : UBUNTU._device-info._tcp.local.
Port number : 0

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 97% of the vulnerabilities on the network.

| Action to take | Vulns | Hosts |
|---|-------|-------|
| Ubuntu 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-6074-1): Update the affected packages. | 262 | 1 |
| Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-7334-1): Update the affected packages. | 262 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7088-1): Update the affected kernel package. | 162 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7391-1): Update the affected kernel package. | 153 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6896-1): Update the affected kernel package. | 149 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7293-1): Update the affected kernel package. | 145 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-5270-1): Update the affected packages. | 133 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Thunderbird vulnerabilities (USN-6015-1): Update the affected packages. | 109 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7516-1): Update the affected kernel package. | 90 | 1 |
| Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-7003-1): Update the affected kernel package. | 85 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1): Update the affected kernel package. | 83 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : MySQL vulnerabilities (USN-5823-1): Update the affected packages. | 77 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-5393-1): Update the affected packages. | 77 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4716-1): Update the affected packages. | 73 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4926-1): Update the affected packages. | 60 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6026-1): Update the affected packages. | 59 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6767-1): Update the affected kernel package. | 48 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6840-1): Update the affected packages. | 47 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6831-1): Update the affected kernel package. | 42 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities (USN-6891-1): Update the affected packages. | 41 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : MariaDB vulnerabilities (USN-5739-1): Update the affected packages. | 36 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6405-1): Update the affected packages. | 33 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7585-1): Update the affected kernel package. | 32 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5923-1): Update the affected packages. | 31 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : MySQL vulnerabilities (USN-7245-1): Update the affected packages. | 31 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-5087-1): Update the affected packages. | 30 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6420-1): Update the affected packages. | 28 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : WebKitGTK vulnerabilities (USN-5893-1): Update the affected packages. | 28 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6557-1): Update the affected packages. | 27 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : MySQL vulnerabilities (USN-7479-1): Update the affected packages. | 27 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-4469-1): Update the affected packages. | 26 | 1 |

| | | |
|---|----|---|
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerabilities (USN-5964-1): Update the affected packages. | 25 | 1 |
| Ubuntu 20.04 LTS : Thunderbird vulnerabilities (USN-4995-1): Update the affected packages. | 25 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thunderbird vulnerabilities (USN-6563-1): Update the affected packages. | 24 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6726-1): Update the affected kernel package. | 23 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7159-1): Update the affected kernel package. | 23 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Exempi vulnerabilities (USN-5483-1): Update the affected packages. | 22 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MySQL vulnerabilities (USN-6615-1): Update the affected packages. | 22 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Good Plugins vulnerabilities (USN-7176-1): Update the affected packages. | 22 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-5043-1): Update the affected packages. | 20 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities (USN-6060-1): Update the affected packages. | 20 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5467-1): Update the affected kernel package. | 20 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1): Update the affected kernel package. | 20 | 1 |
| Ubuntu 20.04 LTS : WebKitGTK vulnerabilities (USN-5394-1): Update the affected packages. | 19 | 1 |
| Ubuntu 20.04 LTS : Samba vulnerabilities (USN-5936-1): Update the affected packages. | 18 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4474-1): Update the affected packages. | 17 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Thunderbird vulnerability (USN-7193-1): Update the affected packages. | 17 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6284-1): Update the affected kernel package. | 16 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-5333-1): Update the affected packages. | 16 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7173-1): Update the affected kernel package. | 16 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Expat vulnerabilities and regression (USN-5320-1): Update the affected packages. | 15 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5000-1): Update the affected kernel package. | 15 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : MySQL vulnerabilities (USN-6934-1): Update the affected packages. | 15 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Samba vulnerabilities (USN-5993-1): Update the affected packages. | 15 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4744-1): Update the affected packages. | 14 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : MySQL vulnerabilities (USN-6459-1): Update the affected packages. | 14 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : MySQL vulnerabilities (USN-6823-1): Update the affected packages. | 14 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6655-1): Update the affected packages. | 14 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-5077-1): Update the affected packages. | 13 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4483-1): Update the affected kernel package. | 13 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4982-1): Update the affected kernel package. | 13 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5338-1): Update the affected kernel package. | 13 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Ghostscript vulnerabilities (USN-7378-1): Update the affected packages. | 13 | 1 |
| Ubuntu 20.04 LTS : MariaDB vulnerabilities (USN-5305-1): Update the affected packages. | 13 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : GNU C Library vulnerabilities (USN-5310-1): Update the affected packages. | 12 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerability (USN-6428-1): Update the affected packages. | 11 | 1 |

| | | |
|---|----|---|
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6270-1): Update the affected packages. | 11 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libsoup vulnerabilities (USN-7543-1): Update the affected packages. | 11 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pillow vulnerabilities (USN-4763-1): Update the affected packages. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : BusyBox vulnerabilities (USN-5179-1): Update the affected packages. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4658-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5562-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5668-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5728-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7461-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7671-1): Update the affected kernel package. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Pillow vulnerability (USN-5227-3): Update the affected packages. | 11 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : libwebp vulnerabilities (USN-4971-1): Update the affected packages. | 11 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : MySQL vulnerabilities (USN-6288-1): Update the affected packages. | 11 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : FreeRDP vulnerabilities (USN-6752-1): Update the affected packages. | 11 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : elfutils vulnerabilities (USN-6322-1): Update the affected packages. | 10 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5849-1): Update the affected packages. | 10 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : FreeRDP vulnerabilities (USN-6401-1): Update the affected packages. | 10 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6548-1): Update the affected kernel package. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeRDP vulnerabilities (USN-5734-1): Update the affected packages. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerability (USN-5612-1): Update the affected intel-microcode package. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerability (USN-5986-1): Update the affected packages. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-4481-1): Update the affected packages. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4750-1): Update the affected kernel package. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5137-1): Update the affected kernel package. | 10 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7022-1): Update the affected kernel package. | 10 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : X.Org X Server vulnerabilities (USN-6587-1): Update the affected packages. | 10 | 1 |
| Ubuntu 20.04 LTS : Ceph vulnerabilities (USN-4998-1): Update the affected packages. | 10 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5963-1): Update the affected packages. | 9 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5147-1): Update the affected packages. | 9 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1): Update the affected intel-microcode package. | 9 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6340-1): Update the affected kernel package. | 9 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6441-1): Update the affected kernel package. | 9 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apport vulnerability (USN-6018-1): Update the affected packages. | 9 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NTFS-3G vulnerability (USN-5711-1): Update the affected packages. | 9 | 1 |

| | | |
|---|---|---|
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6973-1): Update the affected kernel package. | 9 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Samba vulnerabilities (USN-6425-1): Update the affected packages. | 9 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : X.Org X Server vulnerabilities (USN-7299-1): Update the affected packages. | 9 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Ghostscript vulnerabilities (USN-7623-1): Update the affected packages. | 8 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Intel Microcode vulnerabilities (USN-7535-1): Update the affected intel-microcode package. | 8 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Dnsmasq vulnerabilities (USN-4698-1): Update the affected packages. | 8 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GRUB 2 vulnerabilities (USN-4432-1): Update the affected packages. | 8 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : sane-backends vulnerabilities (USN-4470-1): Update the affected packages. | 8 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Net-SNMP vulnerabilities (USN-5795-1): Update the affected packages. | 8 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5415-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5756-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6681-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-1): Update the affected packages. | 8 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6172-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5294-1): Update the affected kernel package. | 8 | 1 |
| Ubuntu 20.04 LTS : OpenJPEG vulnerabilities (USN-4685-1): Update the affected packages. | 8 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5487-1): Update the affected packages. | 7 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-5555-1): Update the affected packages. | 7 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Intel Microcode vulnerabilities (USN-7033-1): Update the affected intel-microcode package. | 7 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Vino vulnerabilities (USN-4573-1): Update the affected vino package. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : Thunderbird vulnerabilities (USN-6075-1): Update the affected packages. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4945-1): Update the affected kernel package. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5210-1): Update the affected kernel package. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1): Update the affected kernel package. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1): Update the affected kernel package. | 7 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6924-1): Update the affected kernel package. | 7 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU binutils vulnerabilities (USN-7423-1): Update the affected packages. | 7 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GStreamer Base Plugins vulnerabilities (USN-7175-1): Update the affected packages. | 7 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : GLib vulnerabilities (USN-6165-1): Update the affected packages. | 7 | 1 |
| Ubuntu 20.04 LTS : Vim regression (USN-5613-2): Update the affected packages. | 7 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : rsync vulnerabilities (USN-7206-1): Update the affected rsync package. | 6 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-4898-1): Update the affected packages. | 6 | 1 |

| | | |
|---|---|---|
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6417-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Bind vulnerabilities (USN-5626-1): Update the affected packages. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibreOffice vulnerabilities (USN-5694-1): Update the affected packages. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : BlueZ vulnerabilities (USN-5155-1): Update the affected packages. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4576-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4679-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4887-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5091-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5116-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5514-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5622-1): Update the affected kernel package. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : MariaDB vulnerabilities (USN-4603-1): Update the affected packages. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : WebKitGTK vulnerabilities (USN-4444-1): Update the affected packages. | 6 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-5079-1): Update the affected packages. | 6 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Avahi vulnerabilities (USN-6487-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : poppler vulnerabilities (USN-6508-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : GNU binutils vulnerabilities (USN-6101-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ncurses vulnerabilities (USN-6099-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5421-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7149-1): Update the affected intel-microcode package. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenJPEG vulnerabilities (USN-7223-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : libsoup vulnerabilities (USN-7643-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : gdb vulnerabilities (USN-6842-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apache HTTP Server vulnerabilities (USN-4458-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4468-1): Update the affected packages. | 5 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4930-1): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6317-1): Update the affected kernel package. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : eSpeak NG vulnerabilities (USN-6858-1): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Apache HTTP Server vulnerabilities (USN-5942-1): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : DjVuLibre vulnerabilities (USN-4957-1): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : LibRaw vulnerabilities (USN-5715-1): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-5523-2): Update the affected packages. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4525-1): Update the affected kernel package. | 5 | 1 |

| | | |
|--|---|---|
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5071-1): Update the affected kernel package. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1): Update the affected kernel package. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6741-1): Update the affected kernel package. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7234-1): Update the affected kernel package. | 5 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Vim vulnerabilities (USN-5247-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6565-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : WebKitGTK vulnerabilities (USN-6061-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Ghostscript vulnerabilities (USN-6835-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7432-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Ghostscript vulnerabilities (USN-6897-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Python vulnerabilities (USN-7015-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerability (USN-7025-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS : Bind vulnerabilities (USN-6642-1): Update the affected packages. | 5 | 1 |
| Ubuntu 20.04 LTS : LibreOffice vulnerabilities (USN-5661-1): Update the affected packages. | 5 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server vulnerabilities (USN-6721-1): Update the affected packages. | 4 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1): Update the affected klibc-utils, libklibc and / or libklibc-dev packages. | 4 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 20.04 LTS : Python vulnerabilities (USN-7348-1): Update the affected packages. | 4 | 1 |
| Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS : Libcroco vulnerabilities (USN-6958-1): Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages. | 4 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Intel Microcode vulnerabilities (USN-5886-1): Update the affected intel-microcode package. | 4 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4985-1): Update the affected intel-microcode package. | 4 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1): Update the affected klibc-utils, libklibc and / or libklibc-dev packages. | 4 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libsepol vulnerabilities (USN-5391-1): Update the affected libsepol1, libsepol1-dev and / or sepol-utils packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1): Update the affected packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1): Update the affected packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : LibRaw vulnerabilities (USN-7485-1): Update the affected packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4929-1): Update the affected packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-4476-1): Update the affected packages. | 4 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4490-1): Update the affected packages. | 4 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6462-1): Update the affected kernel package. | 4 | 1 |

| | | |
|--|---|---|
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6605-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6625-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ceph vulnerabilities (USN-6063-1): Update the affected packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : FreeType vulnerabilities (USN-5528-1): Update the affected packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : NSS vulnerabilities (USN-5892-1): Update the affected libnss3, libnss3-dev and / or libnss3-tools packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Sudo vulnerabilities (USN-6005-1): Update the affected sudo and / or sudo-ldap packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4878-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4909-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5163-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5318-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5691-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6648-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6702-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6776-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7073-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : SPICE vdagent vulnerabilities (USN-4617-1): Update the affected spice-vdagent package. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : X.Org X Server vulnerabilities (USN-5193-1): Update the affected packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : libjpeg-turbo vulnerabilities (USN-5631-1): Update the affected packages. | 4 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : snapd vulnerabilities (USN-5292-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Bind vulnerabilities (USN-6390-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libXpm vulnerabilities (USN-6408-1): Update the affected libxpm-dev, libxpm4 and / or xpmutils packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libx11 vulnerabilities (USN-6407-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerabilities (USN-7314-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerability (USN-7504-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Bind vulnerabilities (USN-6909-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : BusyBox vulnerabilities (USN-6961-1): Update the affected packages. | 4 | 1 |
| Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1): Update the affected kernel package. | 4 | 1 |
| Ubuntu 20.04 LTS : libarchive vulnerability (USN-5374-1): Update the affected libarchive-dev, libarchive-tools and / or libarchive13 packages. | 4 | 1 |
| Ubuntu 20.04 LTS : snapd vulnerabilities (USN-5292-2): Update the affected packages. | 4 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Vim vulnerabilities (USN-7419-1): Update the affected packages. | 3 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerability (USN-7542-1): Update the affected packages. | 3 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : libarchive vulnerabilities (USN-7070-1): Update the affected packages. | 3 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 : LibTIFF vulnerabilities (USN-6644-1): Update the affected packages. | 3 | 1 |

| | | |
|--|---|---|
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 24.04 LTS : Expat vulnerabilities (USN-7000-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : urllib3 vulnerabilities (USN-6473-1): Update the affected python-urllib3 and / or python3-urllib3 packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Intel Microcode vulnerabilities (USN-6286-1): Update the affected intel-microcode package. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Vim vulnerabilities (USN-6154-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : DBus vulnerabilities (USN-5704-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : FLAC vulnerabilities (USN-5733-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5996-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5485-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : systemd vulnerabilities (USN-5928-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : unzip vulnerabilities (USN-5673-1): Update the affected unzip package. | 3 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-5342-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : GifLIB vulnerabilities (USN-6824-1): Update the affected giflib-tools, libgif-dev and / or libgif7 packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Intel Microcode vulnerabilities (USN-7269-1): Update the affected intel-microcode package. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : AccountsService vulnerabilities (USN-4616-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4449-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4720-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Aptdaemon vulnerabilities (USN-4664-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GLib vulnerability (USN-4764-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-1): Update the affected intel-microcode package. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PEAR vulnerability (USN-4723-1): Update the affected php-pear package. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Perl vulnerabilities (USN-4602-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Whoopsie vulnerabilities (USN-4450-1): Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : X.Org X Server vulnerability (USN-4905-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : p11-kit vulnerabilities (USN-4677-1): Update the affected packages. | 3 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4757-1): Update the affected packages. | 3 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6387-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7126-1): Update the affected packages. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : CUPS vulnerabilities (USN-5454-1): Update the affected packages. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Protocol Buffers vulnerabilities (USN-5945-1): Update the affected packages. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : libXpm vulnerabilities (USN-5807-1): Update the affected libxpm-dev, libxpm4 and / or xpmutils packages. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-5332-1): Update the affected packages. | 3 | 1 |

| | | |
|--|---|---|
| Ubuntu 18.04 LTS / 20.04 LTS : FriBidi vulnerabilities (USN-5366-1): Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 packages. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4628-3): Update the affected intel-microcode package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4689-2): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4917-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5017-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5045-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5267-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5384-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5442-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6868-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7408-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7495-1): Update the affected kernel package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : OpenVPN vulnerability (USN-5347-1): Update the affected openvpn package. | 3 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-5615-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Apache HTTP Server vulnerabilities (USN-6506-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : FreeRDP vulnerabilities (USN-6522-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerabilities (USN-6593-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerabilities (USN-6592-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6391-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : YAJL vulnerabilities (USN-6233-2): Update the affected libyajl-dev, libyajl2 and / or yajl-tools packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache HTTP Server vulnerabilities (USN-6729-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Dnsmasq vulnerabilities (USN-6657-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1): Update the affected libnss3, libnss3-dev and / or libnss3-tools packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : TeX Live vulnerabilities (USN-6695-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : SQLite vulnerabilities (USN-7528-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Raptor vulnerabilities (USN-7316-1): Update the affected libraptor2-0, libraptor2-dev and / or raptor2-utils packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : wpa_supplicant and hostapd vulnerabilities (USN-7317-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : snapd vulnerabilities (USN-6940-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Bind vulnerabilities (USN-5827-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerability (USN-7218-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS : GDK-PixBuf vulnerability (USN-5554-1): Update the affected packages. | 3 | 1 |
| Ubuntu 20.04 LTS : GnuTLS vulnerabilities (USN-5029-1): Update the affected packages. | 3 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Requests vulnerabilities (USN-7568-1): Update the affected python-requests, python-requests-whl and / or python3-requests packages. | 2 | 1 |

| | | |
|--|---|---|
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerabilities (USN-6993-1): Update the affected packages. | 2 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-7679-1): Update the affected packages. | 2 | 1 |
| Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libsndfile vulnerabilities (USN-7273-1): Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : AMD Microcode vulnerability (USN-6319-1): Update the affected amd64-microcode package. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-6512-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : Ghostscript vulnerabilities (USN-6364-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : poppler vulnerabilities (USN-6299-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Dnsmasq vulnerability (USN-6034-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Kerberos vulnerabilities (USN-5828-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-5960-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : X.Org X Server vulnerabilities (USN-5740-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libcaca vulnerabilities (USN-5119-1): Update the affected caca-utils, libcaca-dev and / or libcaca0 packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : urllib3 vulnerabilities (USN-7599-1): Update the affected python-urllib3 and / or python3-urllib3 packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : GDK-PixBuf vulnerabilities (USN-7662-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-6809-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GStreamer Good Plugins vulnerabilities (USN-4928-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibTIFF vulnerabilities (USN-4755-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-4591-1): Update the affected kernel package. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Net-SNMP vulnerabilities (USN-4471-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PackageKit vulnerabilities (USN-4538-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Pygments vulnerability (USN-4897-1): Update the affected python-pygments and / or python3-pygments packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-4754-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Sudo vulnerabilities (USN-4705-1): Update the affected sudo and / or sudo-ldap packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ldb vulnerabilities (USN-4888-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libproxy vulnerability (USN-4673-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libx11 vulnerabilities (USN-4487-1): Update the affected packages. | 2 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : tar vulnerabilities (USN-4692-1): Update the affected tar and / or tar-scripts packages. | 2 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-1): Update the affected kernel package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : python-cryptography vulnerabilities (USN-6673-1): Update the affected python-cryptography and / or python3-cryptography packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Python vulnerabilities (USN-7570-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : DHCP vulnerabilities (USN-5658-1): Update the affected packages. | 2 | 1 |

| | | |
|--|---|---|
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerabilities (USN-5638-2): Update the affected expat, libexpat1 and / or libexpat1-dev packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerabilities (USN-5643-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuTLS vulnerabilities (USN-5550-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5476-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libxslt vulnerabilities (USN-5575-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-5767-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : networkd-dispatcher vulnerabilities (USN-5395-1): Update the affected networkd-dispatcher package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Avahi vulnerabilities (USN-5008-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : FreeRDP vulnerabilities (USN-5154-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : GNOME Autoar vulnerability (USN-4937-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : GNU binutils vulnerabilities (USN-5124-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-5224-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Kerberos vulnerabilities (USN-5959-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Libgcrypt vulnerabilities (USN-5080-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : LibreOffice vulnerability (USN-6023-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel update (USN-4689-4): Update the affected kernel package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5358-1): Update the affected kernel package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-5410-1): Update the affected libnss3, libnss3-dev and / or libnss3-tools packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Nettle vulnerabilities (USN-4990-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Perl DBI module vulnerabilities (USN-5030-1): Update the affected libdbi-perl package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : QPDF vulnerabilities (USN-5026-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : Squashfs-Tools vulnerability (USN-5078-1): Update the affected squashfs-tools package. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : libzstd vulnerabilities (USN-4760-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : systemd vulnerabilities (USN-5013-1): Update the affected packages. | 2 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS : tcpdump vulnerabilities (USN-5331-2): Update the affected tcpdump package. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 : curl vulnerabilities (USN-6237-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Open VM Tools vulnerabilities (USN-6463-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Perl vulnerabilities (USN-6517-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : SQLite vulnerabilities (USN-6566-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : curl vulnerabilities (USN-6535-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : python-cryptography vulnerabilities (USN-6539-1): Update the affected python-cryptography and / or python3-cryptography packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : GStreamer Base Plugins vulnerabilities (USN-6268-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : LibRaw vulnerabilities (USN-6137-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : curl vulnerabilities (USN-6429-1): Update the affected packages. | 2 | 1 |

| | | |
|---|---|---|
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libcap2 vulnerabilities (USN-6166-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libssh vulnerabilities (USN-6138-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libvpx vulnerabilities (USN-6403-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : poppler vulnerabilities (USN-6273-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : OpenVPN vulnerabilities (USN-6860-1): Update the affected openvpn package. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : MariaDB vulnerabilities (USN-6600-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerabilities (USN-6618-1): Update the affected python3-pil and / or python3-pil.imagetk packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libarchive vulnerabilities (USN-7454-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Bind vulnerabilities (USN-7241-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Libxslt vulnerability (USN-7361-1): Update the affected libxslt1-dev, libxslt1.1 and / or xsltproc packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenSSH vulnerabilities (USN-7270-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Python vulnerability (USN-7280-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerabilities (USN-7426-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-7012-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : libgsf vulnerabilities (USN-7062-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : BlueZ vulnerabilities (USN-7222-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : HarfBuzz vulnerability (USN-7251-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : Pillow vulnerabilities (USN-5777-1): Update the affected python3-pil and / or python3-pil.imagetk packages. | 2 | 1 |
| Ubuntu 20.04 LTS / 22.04 LTS : cups-filters vulnerabilities (USN-7043-4): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS : GUPnP vulnerability (USN-4970-1): Update the affected gir1.2-gupnp-1.2, libgupnp-1.2-0 and / or libgupnp-1.2-dev packages. | 2 | 1 |
| Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5589-1): Update the affected kernel package. | 2 | 1 |
| Ubuntu 20.04 LTS : PolicyKit vulnerability (USN-5304-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS : Python vulnerabilities (USN-5201-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS : cryptsetup vulnerability (USN-5286-1): Update the affected packages. | 2 | 1 |
| Ubuntu 20.04 LTS : libuv vulnerability (USN-5007-1): Update the affected libuv1 and / or libuv1-dev packages. | 2 | 1 |
| Ubuntu 20.04 LTS : util-linux vulnerabilities (USN-5279-1): Update the affected packages. | 2 | 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 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1): Update the affected packages. | 1 | 1 |

| | | |
|--|---|---|
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1): Update the affected less package. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerability (USN-6744-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Setuptools vulnerability (USN-7544-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Expat vulnerability (USN-7145-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Kerberos vulnerability (USN-7257-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Setuptools vulnerability (USN-7002-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : wpa_supplicant and hostapd vulnerability (USN-6945-1): Update the affected packages. | 1 | 1 |
| Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libxslt vulnerability (USN-7600-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : BlueZ vulnerability (USN-6540-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1): Update the affected tar and / or tar-scripts packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Intel Microcode vulnerability (USN-6485-1): Update the affected intel-microcode package. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libsndfile vulnerability (USN-6471-1): Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : procps-ng vulnerability (USN-6477-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Ghostscript vulnerability (USN-6297-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6257-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6139-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 : Ceph vulnerability (USN-6613-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : gawk vulnerability (USN-6373-1): Update the affected gawk package. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : nghttp2 vulnerability (USN-6142-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : snapd vulnerability (USN-6125-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Expat vulnerability (USN-5638-3): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU binutils vulnerability (USN-5762-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Ghostscript vulnerability (USN-6017-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : jBIG-KIT vulnerability (USN-5742-1): Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5688-1): Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages. | 1 | 1 |

| | | |
|--|---|---|
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Mako vulnerability (USN-5625-1): Update the affected python-mako and / or python3-mako packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM regressions (USN-5825-2): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Perl vulnerability (USN-5689-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Setuptools vulnerability (USN-5817-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : apr-util vulnerability (USN-5870-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : curl vulnerability (USN-5587-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : e2fsprogs vulnerability (USN-5464-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : poppler vulnerability (USN-5606-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : python-future vulnerability (USN-5833-1): Update the affected python-future and / or python3-future packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : shadow vulnerability (USN-5745-1): Update the affected login, passwd and / or uidmap packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : snapd vulnerability (USN-5753-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : tar vulnerability (USN-5900-1): Update the affected tar and / or tar-scripts packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Aspell vulnerability (USN-5023-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1): Update the affected bash, bash-builtins and / or bash-static packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : BlueZ vulnerability (USN-5275-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GMP vulnerability (USN-5672-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GNOME grilo vulnerability (USN-5055-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GStreamer Base Plugins vulnerability (USN-4959-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5493-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Speex vulnerability (USN-5280-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5573-1): Update the affected rsync package. | 1 | 1 |
| Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : tar vulnerability (USN-5329-1): Update the affected tar and / or tar-scripts packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : CUPS vulnerability (USN-6844-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GDK-PixBuf vulnerability (USN-6806-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1): Update the affected pypy-idna, python-idna and / or python3-idna packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1): Update the affected less package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Apport vulnerability (USN-7545-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : libvpx vulnerability (USN-7551-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : AMD Microcode vulnerability (USN-7077-1): Update the affected amd64-microcode package. | 1 | 1 |

| | | |
|--|---|---|
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerability (USN-7213-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : urllib3 vulnerability (USN-7084-1): Update the affected python-urllib3 and / or python3-urllib3 packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : APR vulnerability (USN-7038-1): Update the affected libapr1, libapr1-dev and / or libapr1t64 packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : GLib vulnerability (USN-7114-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : LibTIFF vulnerability (USN-6997-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJPEG vulnerability (USN-7037-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Vim vulnerability (USN-7048-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : nano vulnerability (USN-7064-1): Update the affected nano and / or nano-tiny packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : APT vulnerability (USN-4667-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Brotli vulnerability (USN-4568-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : File Roller vulnerability (USN-4927-1): Update the affected file-roller package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : FreeType vulnerability (USN-4593-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Kerberos vulnerability (USN-4635-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer, Vino vulnerability (USN-4636-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4489-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4627-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-4694-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Nettle vulnerability (USN-4906-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PulseAudio vulnerability (USN-4640-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Raptor vulnerability (USN-4630-1): Update the affected libraptor2-0, libraptor2-dev and / or libraptor2-utils packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Samba vulnerability (USN-4454-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Software Properties vulnerability (USN-4457-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerability (USN-4466-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libcaca vulnerability (USN-4921-1): Update the affected caca-utils, libcaca-dev and / or libcaca0 packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif vulnerability (USN-4624-1): Update the affected libexif-dev and / or libexif12 packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libfcgi-perl vulnerability (USN-7527-1): Update the affected libfcgi-perl package. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libssh vulnerability (USN-4447-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ppp vulnerability (USN-4451-1): Update the affected ppp, ppp-dev and / or ppp-udeb packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-apt vulnerability (USN-4668-1): Update the affected packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : python-cryptography vulnerability (USN-4613-1): Update the affected python-cryptography and / or python3-cryptography packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : snapd vulnerability (USN-4728-1): Update the affected packages. | 1 | 1 |

| | | |
|---|---|---|
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : urllib3 vulnerability (USN-4570-1): Update the affected python-urllib3 and / or python3-urllib3 packages. | 1 | 1 |
| Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils vulnerability (USN-4649-1): Update the affected xdg-utils package. | 1 | 1 |
| Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1): Update the affected kernel package. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : CUPS vulnerability (USN-6128-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : TeX Live vulnerability (USN-6115-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : cups-filters vulnerability (USN-6083-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6078-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : poppler vulnerabilities (USN-7471-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : GNU C Library vulnerability (USN-7259-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNOME Files vulnerability (USN-5786-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GNU C Library vulnerability (USN-7541-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : GnuPG vulnerability (USN-5503-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : HTTP-Daemon vulnerability (USN-5520-1): Update the affected libhttp-daemon-perl package. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerability (USN-5743-2): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5787-1): Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Open VM Tools vulnerability (USN-5578-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-5424-1): Update the affected packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : PyJWT vulnerability (USN-5526-1): Update the affected python-jwt and / or python3-jwt packages. | 1 | 1 |
| Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Rsyslog vulnerability (USN-5404-1): Update the affected packages. | 1 | 1 |

© 2025 Tenable™, Inc. All rights reserved.