



Photographer

Sat, 01 Nov 2025 19:40:40 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.84.42.93

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

- Suggested Remediations

Vulnerabilities by Host

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

10.84.42.93

43

283

452

71

134

CRITICAL

HIGH

MEDIUM

LOW

INFO

Scan Information

Start time: Sat Nov 1 19:24:15 2025

End time: Sat Nov 1 19:40:39 2025

Host Information

Netbios Name: PHOTOGRAPHER

IP: 10.84.42.93

MAC Address: 08:00:27:0A:3B:E9

OS: Linux Kernel 4.15.0-45-generic on Ubuntu 16.04

Vulnerabilities

201351 - Canonical Ubuntu Linux SEoL (16.04.x)

Synopsis

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

Description

According to its version, Canonical Ubuntu Linux is 16.04.x. It is, therefore, no longer maintained by its vendor or provider.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

<http://www.nessus.org/u?cd15280>

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 16.04.6 LTS (Xenial Xerus)
Security End of Life : April 30, 2021
Time since Security End of Life (Est.) : >= 4 years
```

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_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm2

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

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 : libarchive13_3.1.2-11ubuntu0.16.04.6
- Fixed package : libarchive13_3.1.2-11ubuntu0.16.04.8+esm1

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

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 : rsync_3.1.1-3ubuntu1.2
- Fixed package : rsync_3.1.1-3ubuntu1.3+esm3

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: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

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 : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm9

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/VC: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_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5+esm3

240197 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Samba vulnerabilities (USN-7582-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7582-1 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)

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)

Florent Saudel 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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7582-1>

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-2022-3437
CVE	CVE-2022-42898
CVE	CVE-2022-45141
CVE	CVE-2023-34966
XREF	IAVA:2022-A-0447-S
XREF	IAVA:2022-A-0495-S
XREF	IAVA:2023-A-0004-S
XREF	IAVA:2023-A-0376-S
XREF	USN:7582-1

Plugin Information

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

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.

- Installed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2
- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm2

181560 - Ubuntu 16.04 ESM / 18.04 ESM : GNU binutils vulnerabilities (USN-6381-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6381-1 advisory.

It was discovered that a memory leak existed in certain GNU binutils modules. An attacker could possibly use this issue to cause a denial of service (memory exhaustion). (CVE-2020-19724, CVE-2020-21490)

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-2020-19726, CVE-2021-46174, CVE-2022-45703)

It was discovered that GNU binutils was not properly initializing heap memory when processing certain print instructions. An attacker could possibly use this issue to expose sensitive information.

(CVE-2020-35342)

It was discovered that GNU binutils was not properly handling the logic behind certain memory management related operations, which could lead to a buffer

overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-44840)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6381-1>

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-2020-19724
CVE	CVE-2020-19726
CVE	CVE-2020-21490
CVE	CVE-2020-35342
CVE	CVE-2021-46174
CVE	CVE-2022-44840
CVE	CVE-2022-45703
CVE	CVE-2022-47695
XREF	USN:6381-1

Plugin Information

Published: 2023/09/18, 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.

- Installed package : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm7

179075 - Ubuntu 16.04 ESM / 18.04 ESM : OpenSSH vulnerability (USN-6242-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6242-2 advisory.

USN-6242-1 fixed a vulnerability in OpenSSH. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6242-2>

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)

STIG Severity

I

References

CVE	CVE-2023-38408
XREF	USN:6242-2
XREF	IAVA:2023-A-0377-S

Plugin Information

Published: 2023/07/31, Modified: 2024/10/29

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 : `openssh-client_1:7.2p2-4ubuntu2.10`
- Fixed package : `openssh-client_1:7.2p2-4ubuntu2.10+esm3`
- Installed package : `openssh-server_1:7.2p2-4ubuntu2.10`
- Fixed package : `openssh-server_1:7.2p2-4ubuntu2.10+esm3`
- Installed package : `openssh-sftp-server_1:7.2p2-4ubuntu2.10`
- Fixed package : `openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm3`

181129 - Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerability (USN-6354-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6354-1 advisory.

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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6354-1>

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-2022-48565
XREF	USN:6354-1

Plugin Information

Published: 2023/09/07, 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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm6
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm6
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm6
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm9
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm9
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm9
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm6
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm6
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm9
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm9

189293 - Ubuntu 16.04 ESM / 18.04 ESM : X.Org X Server vulnerabilities (USN-6587-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6587-2 advisory.

USN-6587-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6587-2>

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-2023-6816
CVE	CVE-2024-0229
CVE	CVE-2024-0408
CVE	CVE-2024-0409
CVE	CVE-2024-21885
CVE	CVE-2024-21886
XREF	USN:6587-2

Plugin Information

Published: 2024/01/22, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm9

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: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

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 : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.54.3+16.04.0ubuntu0.1~esm6
- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.54.3+16.04.0ubuntu0.1~esm6

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

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_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.14+esm5
- Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.14+esm5
- Installed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.14+esm5
- Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.14+esm5

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

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 : libksba8_1.3.3-1ubuntu0.16.04.1
- Fixed package : libksba8_1.3.3-1ubuntu0.16.04.1+esm1

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: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:5825-2

Plugin Information

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

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 : libpam-modules_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm4
- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm4
- Installed package : libpam-runtime_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm4
- Installed package : libpam0g_1.1.8-3.2ubuntu2.1
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm4

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	CVE-2022-28321
XREF	USN:5825-1

Plugin Information

Published: 2023/01/25, 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.

- Installed package : libpam-modules_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm2
- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm2
- Installed package : libpam-runtime_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm2
- Installed package : libpam0g_1.1.8-3.2ubuntu2.1
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm2

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: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

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 : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

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

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 : rsync_3.1.1-3ubuntu1.2
- Fixed package : rsync_3.1.1-3ubuntu1.3+esm2

164275 - Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5570-1 advisory.

Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate 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-5570-1>

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-2022-37434
USN:5570-1

Plugin Information

Published: 2022/08/18, 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.

- Installed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.1
- Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3+esm2

173277 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerability (USN-5942-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5942-2 advisory.

USN-5942-1 fixed vulnerabilities in Apache HTTP Server. This update provides the corresponding update for CVE-2023-25690 for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5942-2>

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)

STIG Severity

I

References

CVE	CVE-2023-25690
XREF	USN:5942-2
XREF	IAVA:2023-A-0124-S

Plugin Information

Published: 2023/03/22, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm10
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm10
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm10
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm10

168184 - Ubuntu 16.04 ESM : LibTIFF vulnerability (USN-5743-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5743-1 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-5743-1>

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-2022-3970
XREF	USN:5743-1

Plugin Information

Published: 2022/11/25, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm8

169707 - Ubuntu 16.04 ESM : Libksba vulnerability (USN-5787-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5787-2 advisory.

USN-5787-1 fixed vulnerabilities in Libksba. This update provides the corresponding updates for Ubuntu 16.04 ESM and Ubuntu 14.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5787-2>

Solution

Update the affected libksba-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: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:5787-2

Plugin Information

Published: 2023/01/09, Modified: 2024/10/29

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 : libksba8_1.3.3-1ubuntu0.16.04.1
- Fixed package : libksba8_1.3.3-1ubuntu0.16.04.1+esm2

171513 - Ubuntu 16.04 ESM : NSS vulnerabilities (USN-5872-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5872-1 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. (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-5872-1>

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-2022-22747
CVE	CVE-2022-34480
XREF	USN:5872-1

Plugin Information

Published: 2023/02/15, 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.

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.14+esm3
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.14+esm3

172223 - Ubuntu 16.04 ESM : NSS vulnerability (USN-5892-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5892-2 advisory.

USN-5892-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5892-2>

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

7.7 (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-2023-0767
XREF	USN:5892-2

Plugin Information

Published: 2023/03/07, Modified: 2024/10/29

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 : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.14+esm4
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.14+esm4

161611 - Ubuntu 16.04 ESM : OpenSSL vulnerabilities (USN-5402-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5402-2 advisory.

USN-5402-1 fixed several vulnerabilities in OpenSSL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5402-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-1292
CVE	CVE-2022-1473
XREF	USN:5402-2
XREF	IAVA:2022-A-0186-S

Plugin Information

Published: 2022/05/27, Modified: 2025/08/12

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 : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm3
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm3

162773 - Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-5488-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5488-2 advisory.

USN-5488-1 fixed vulnerabilities in OpenSSL. This update provides the corresponding updates for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5488-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl 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-2022-2068
XREF	USN:5488-2
XREF	IAVA:2022-A-0257-S

Plugin Information

Published: 2022/07/07, Modified: 2024/11/05

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 : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm5
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm5

173432 - Ubuntu 16.04 ESM : curl vulnerabilities (USN-5964-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5964-2 advisory.

USN-5964-1 fixed several vulnerabilities in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5964-2>

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)

STIG Severity

I

References

CVE	CVE-2023-27533
CVE	CVE-2023-27535
CVE	CVE-2023-27536
XREF	USN:5964-2
XREF	IAVA:2023-A-0153-S

Plugin Information

Published: 2023/03/27, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm8
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm8

166574 - Ubuntu 16.04 ESM : curl vulnerability (USN-5702-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5702-2 advisory.

USN-5702-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5702-2>

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: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
XREF	USN:5702-2
XREF	IAVA:2022-A-0451-S

Plugin Information

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

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm6
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm6

184162 - Ubuntu 16.04 ESM : libvpx vulnerabilities (USN-6403-3)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6403-3 advisory.

USN-6403-1 fixed several vulnerabilities in libvpx. This update provides the corresponding update for Ubuntu 16.04 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-6403-3>

Solution

Update the affected libvpx-dev, libvpx3 and / or vpx-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

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-2023-5217
CVE	CVE-2023-44488
XREF	CISA-KNOWN-EXPLOITED:2023/10/23
XREF	USN:6403-3

Plugin Information

Published: 2023/11/01, Modified: 2024/10/29

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 : libvpx3_1.5.0-2ubuntu1
- Fixed package : libvpx3_1.5.0-2ubuntu1.1+esm2

168311 - Ubuntu 16.04 ESM : pixman vulnerability (USN-5718-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5718-2 advisory.

USN-5718-1 fixed a vulnerability in pixman. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5718-2>

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: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:5718-2

Plugin Information

Published: 2022/11/30, Modified: 2024/10/29

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 : libpixman-1-0_0.33.6-1
- Fixed package : libpixman-1-0_0.33.6-1ubuntu0.1~esm1

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

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 : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.8+esm4
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.8+esm4
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.8+esm4

136545 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox regression (USN-4353-2)**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-4353-2 advisory.

USN-4353-1 fixed vulnerabilities in Firefox. The update caused a regression that impaired the functionality of some addons. 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-4353-2>

Solution

Update the affected packages.

Risk Factor

Critical

STIG Severity

II

References

XREF	USN:4353-2
XREF	IAVA:2020-A-0190-S

Plugin Information

Published: 2020/05/13, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_76.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_76.0.1+build1-0ubuntu0.16.04.1

136420 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4353-1)

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-4353-1 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, bypass security restrictions, spoof the URL bar, or execute arbitrary code. (CVE-2020-6831, CVE-2020-12387, CVE-2020-12390, CVE-2020-12391, CVE-2020-12394, CVE-2020-12395, CVE-2020-12396)

It was discovered that the Devtools Copy as cURL feature did not properly escape the HTTP POST data of a request. If a user were tricked in to using the Copy as cURL feature to copy and paste a command with specially crafted data in to a terminal, an attacker could potentially exploit this to obtain sensitive information from local files. (CVE-2020-12392)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4353-1>

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-2020-12387
CVE	CVE-2020-12390
CVE	CVE-2020-12391
CVE	CVE-2020-12392
CVE	CVE-2020-12394
CVE	CVE-2020-12395
CVE	CVE-2020-12396

CVE CVE-2020-6831
XREF USN:4353-1
XREF IAVA:2020-A-0190-S

Plugin Information

Published: 2020/05/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_76.0+build2-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_76.0+build2-0ubuntu0.16.04.1
```

136894 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-4373-1)

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-4373-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked in to 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-2020-6831, CVE-2020-12387, CVE-2020-12395)

It was discovered that the Devtools Copy as cURL feature did not properly escape the HTTP POST data of a request. If a user were tricked in to using the Copy as CURL feature to copy and paste a command with specially crafted data in to a terminal, an attacker could potentially exploit this to obtain sensitive information from local files. (CVE-2020-12392)

It was discovered that Thunderbird did not correctly handle Unicode whitespace characters within the From email header. An attacker could potentially exploit this to spoof the sender email address that Thunderbird displays. (CVE-2020-12397)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4373-1>

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-2020-12387

CVE	CVE-2020-12392
CVE	CVE-2020-12395
CVE	CVE-2020-12397
CVE	CVE-2020-6831
XREF	USN:4373-1
XREF	IAVA:2020-A-0190-S

Plugin Information

Published: 2020/05/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:68.8.0+build2-0ubuntu0.16.04.2
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:68.8.0+build2-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:68.8.0+build2-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:68.8.0+build2-0ubuntu0.16.04.2

207382 - Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-3)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6885-3 advisory.

USN-6885-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6885-3>

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-2024-38474](https://nvd.nist.gov/vuln/detail/CVE-2024-38474)

CVE	CVE-2024-38475
CVE	CVE-2024-38476
CVE	CVE-2024-38477
XREF	IAVA:2024-A-0378-S
XREF	USN:6885-3
XREF	CISA-KNOWN-EXPLOITED:2025/05/22

Plugin Information

Published: 2024/09/18, Modified: 2025/05/02

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.

- Installed package : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm13
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm13
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm13
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm13

183605 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4032-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4032-1 advisory.

It was discovered that a sandboxed child process could open arbitrary web content in the parent process via the Prompt:Open IPC message. When combined with another vulnerability, 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-4032-1>

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

9.3 (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

II

References

CVE	CVE-2019-11708
XREF	CISA-KNOWN-EXPLOITED:2022/06/13
XREF	IAVA:2019-A-0211-S
XREF	USN:4032-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_67.0.4+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_67.0.4+build1-0ubuntu0.16.04.1

128680 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel regression (USN-4115-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4115-2 advisory.

USN 4115-1 fixed vulnerabilities in the Linux 4.15 kernel for Ubuntu 18.04 LTS and Ubuntu 16.04 LTS.

Unfortunately, as part of the update, a regression was introduced that caused a kernel crash when handling fragmented packets in some situations. This update addresses the issue.

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-4115-2>

Solution

Update the affected kernel package.

Risk Factor

Critical

References

XREF USN:4115-2

Plugin Information

Published: 2019/09/11, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-62-generic for this advisory.

128475 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4115-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4115-1 advisory.

Hui Peng and Mathias Payer discovered that the Option USB High Speed driver in the Linux kernel did not properly validate metadata received from the device. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2018-19985)

Zhipeng Xie discovered that an infinite loop could be triggered in the CFS Linux kernel process scheduler. A local attacker could possibly use this to cause a denial of service. (CVE-2018-20784)

It was discovered that the Intel Wi-Fi device driver in the Linux kernel did not properly validate certain Tunneled Direct Link Setup (TDLS). A physically proximate attacker could use this to cause a denial of service (Wi-Fi disconnect). (CVE-2019-0136)

It was discovered that the Bluetooth UART implementation in the Linux kernel did not properly check for missing tty operations. A local attacker could use this to cause a denial of service. (CVE-2019-10207)

Amit Klein and Benny Pinkas discovered that the Linux kernel did not sufficiently randomize IP ID values generated for connectionless networking protocols. A remote attacker could use this to track particular Linux devices. (CVE-2019-10638)

Amit Klein and Benny Pinkas discovered that the location of kernel addresses could be exposed by the implementation of connection-less network protocols in the Linux kernel. A remote attacker could possibly use this to assist in the exploitation of another vulnerability in the Linux kernel. (CVE-2019-10639)

It was discovered that an integer overflow existed in the Linux kernel when reference counting pages, leading to potential use-after-free issues. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-11487)

Jann Horn discovered that a race condition existed in the Linux kernel when performing core dumps. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2019-11599)

It was discovered that a null pointer dereference vulnerability existed in the LSI Logic MegaRAID driver in the Linux kernel. A local attacker could use this to cause a denial of service (system crash).

(CVE-2019-11810)

It was discovered that the GTC0 tablet input driver in the Linux kernel did not properly bounds check the initial HID report sent by the device. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-13631)

Praveen Pandey discovered that the Linux kernel did not properly validate sent signals in some situations on PowerPC systems with transactional memory disabled. A local attacker could use this to cause a denial of service. (CVE-2019-13648)

It was discovered that the floppy driver in the Linux kernel did not properly validate meta data, leading to a buffer overread. A local attacker could use this to cause a denial of service (system crash).

(CVE-2019-14283)

It was discovered that the floppy driver in the Linux kernel did not properly validate ioctl() calls, leading to a division-by-zero. A local attacker could use this to cause a denial of service (system crash). (CVE-2019-14284)

Tuba Yavuz discovered that a race condition existed in the DesignWare USB3 DRD Controller device driver in the Linux kernel. A physically proximate attacker could use this to cause a denial of service.

(CVE-2019-14763)

It was discovered that an out-of-bounds read existed in the QLogic QEDI iSCSI Initiator Driver in the Linux kernel. A local attacker could possibly use this to expose sensitive information (kernel memory).

(CVE-2019-15090)

It was discovered that the Raremono AM/FM/SW radio device driver in the Linux kernel did not properly allocate memory, leading to a use-after-free. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2019-15211)

It was discovered at a double-free error existed in the USB Rio 500 device driver for the Linux kernel. A physically proximate attacker could use this to cause a denial of service. (CVE-2019-15212)

It was discovered that a race condition existed in the Advanced Linux Sound Architecture (ALSA) subsystem of the Linux kernel, leading to a potential use-after-free. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-15214)

It was discovered that a race condition existed in the CPIA2 video4linux device driver for the Linux kernel, leading to a use-after-free. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-15215)

It was discovered that a race condition existed in the Softmac USB Prism54 device driver in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash).

(CVE-2019-15220)

It was discovered that a use-after-free vulnerability existed in the AppleTalk implementation in the Linux kernel if an error occurs during initialization. A local attacker could use this to cause a denial of service (system crash). (CVE-2019-15292)

Jason Wang discovered that an infinite loop vulnerability existed in the virtio net driver in the Linux kernel. A local attacker in a guest VM could possibly use this to cause a denial of service in the host system. (CVE-2019-3900)

Daniele Antonioli, Nils Ole Tippenhauer, and Kasper B. Rasmussen discovered that the Bluetooth protocol BR/EDR specification did not properly require sufficiently strong encryption key lengths. A physically proximate attacker could use this to expose sensitive information. (CVE-2019-9506)

It was discovered that a race condition existed in the USB YUREX device driver in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15216)

It was discovered that the Siano USB MDTV receiver device driver in the Linux kernel made improper assumptions about the device characteristics. A physically proximate attacker could use this cause a denial of service (system crash). (CVE-2019-15218)

It was discovered that the Line 6 POD USB device driver in the Linux kernel did not properly validate data size information from the device. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15221)

Muyu Yu discovered that the CAN implementation in the Linux kernel in some situations did not properly restrict the field size when processing outgoing frames. A local attacker with CAP_NET_ADMIN privileges could use this to execute arbitrary code. (CVE-2019-3701)

Vladis Dronov discovered that the debug interface for the Linux kernel's HID subsystem did not properly validate passed parameters in some situations. A local privileged attacker could use this to cause a denial of service (infinite loop). (CVE-2019-3819)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4115-1>

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

8.8 (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-2018-19985
CVE	CVE-2018-20784
CVE	CVE-2019-0136
CVE	CVE-2019-10207
CVE	CVE-2019-10638
CVE	CVE-2019-10639
CVE	CVE-2019-11487
CVE	CVE-2019-11599
CVE	CVE-2019-11810
CVE	CVE-2019-13631
CVE	CVE-2019-13648
CVE	CVE-2019-14283
CVE	CVE-2019-14284
CVE	CVE-2019-14763
CVE	CVE-2019-15090
CVE	CVE-2019-15211
CVE	CVE-2019-15212
CVE	CVE-2019-15214
CVE	CVE-2019-15215
CVE	CVE-2019-15216
CVE	CVE-2019-15218
CVE	CVE-2019-15220
CVE	CVE-2019-15221
CVE	CVE-2019-15292
CVE	CVE-2019-3701
CVE	CVE-2019-3819

CVE	CVE-2019-3900
CVE	CVE-2019-9506
XREF	USN:4115-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/09/03, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-60-generic for this advisory.

130151 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4162-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4162-1 advisory.

It was discovered that the RSI 91x Wi-Fi driver in the Linux kernel did not handle detach operations correctly, 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-2018-21008)

Wen Huang discovered that the Marvell Wi-Fi device driver in the Linux kernel did not properly perform bounds checking, leading to a heap overflow. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-14814, CVE-2019-14815, CVE-2019-14816)

Matt Delco discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform bounds checking when handling coalesced MMIO write operations. A local attacker with write access to /dev/kvm could use this to cause a denial of service (system crash). (CVE-2019-14821)

Hui Peng and Mathias Payer discovered that the USB audio driver for the Linux kernel did not properly validate device meta data. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15117)

Hui Peng and Mathias Payer discovered that the USB audio driver for the Linux kernel improperly performed recursion while handling device meta data. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15118)

It was discovered that the Technisat DVB-S/S2 USB device driver in the Linux kernel contained a buffer overread. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2019-15505)

Brad Spengler discovered that a Spectre mitigation was improperly implemented in the ptrace subsystem of the Linux kernel. A local attacker could possibly use this to expose sensitive information.

(CVE-2019-15902)

It was discovered that the SMB networking file system implementation in the Linux kernel contained a buffer overread. An attacker could use this to expose sensitive information (kernel memory).

(CVE-2019-15918)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4162-1>

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

8.8 (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-2018-21008
CVE	CVE-2019-14814
CVE	CVE-2019-14815
CVE	CVE-2019-14816
CVE	CVE-2019-14821
CVE	CVE-2019-15117
CVE	CVE-2019-15118
CVE	CVE-2019-15505
CVE	CVE-2019-15902
CVE	CVE-2019-15918
XREF	USN:4162-1

Plugin Information

Published: 2019/10/22, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-66-generic for this advisory.
```

132691 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4227-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4227-1 advisory.

It was discovered that a heap-based buffer overflow existed in the Marvell WiFi-Ex Driver for the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-14895, CVE-2019-14901)

It was discovered that a heap-based buffer overflow existed in the Marvell Libertas WLAN Driver for the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-14896, CVE-2019-14897)

It was discovered that the Fujitsu ES network device driver for the Linux kernel did not properly check for errors in some situations, leading to a NULL pointer dereference. A local attacker could use this to cause a denial of service. (CVE-2019-16231)

It was discovered that the QLogic Fibre Channel driver in the Linux kernel did not properly check for error, leading to a NULL pointer dereference. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-16233)

Anthony Steinhauser discovered that the Linux kernel did not properly perform Spectre_RSB mitigations to all processors for PowerPC architecture systems in some situations. A local attacker could use this to expose sensitive information. (CVE-2019-18660)

It was discovered that the Mellanox Technologies Innova driver in the Linux kernel did not properly deallocate memory in certain failure conditions. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19045)

It was discovered that Geschwister Schneider USB CAN interface driver in the Linux kernel did not properly deallocate memory in certain failure conditions. A physically proximate attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19052)

It was discovered that the AMD Display Engine Driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attack could use this to cause a denial of service (memory exhaustion). (CVE-2019-19083)

It was discovered that the driver for memoryless force-feedback input devices in the Linux kernel contained a use-after-free vulnerability. A physically proximate attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2019-19524)

It was discovered that the Microchip CAN BUS Analyzer driver in the Linux kernel contained a use-after-free vulnerability on device disconnect. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-19529)

It was discovered that the PEAK-System Technik USB driver in the Linux kernel did not properly sanitize memory before sending it to the device. A physically proximate attacker could use this to expose sensitive information (kernel memory). (CVE-2019-19534)

Tristan Madani discovered that the ALSA timer 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-2019-19807)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4227-1>

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

8.8 (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-2019-14895
CVE	CVE-2019-14896
CVE	CVE-2019-14897
CVE	CVE-2019-14901
CVE	CVE-2019-16231
CVE	CVE-2019-16233
CVE	CVE-2019-18660
CVE	CVE-2019-19045
CVE	CVE-2019-19052
CVE	CVE-2019-19083
CVE	CVE-2019-19524
CVE	CVE-2019-19529
CVE	CVE-2019-19534
CVE	CVE-2019-19807
XREF	USN:4227-1

Plugin Information

Published: 2020/01/07, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-74-generic for this advisory.

207588 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7028-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7028-1 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).

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;

- Greybus drivers;
- Modular ISDN driver;
- Multiple devices driver;
- Network drivers;
- SCSI drivers;
- VFIO drivers;
- F2FS file system;
- GFS2 file system;
- JFS file system;
- NILFS2 file system;
- Kernel debugger infrastructure;
- Bluetooth subsystem;
- IPv4 networking;
- L2TP protocol;
- Netfilter;

- RxRPC session sockets; (CVE-2024-42154, CVE-2023-52527, CVE-2024-26733, CVE-2024-42160, CVE-2021-47188, CVE-2024-38570, CVE-2024-26851, CVE-2024-26984, CVE-2024-26677, CVE-2024-39480, CVE-2024-27398, CVE-2022-48791, CVE-2024-42224, CVE-2024-38583, CVE-2024-40902, CVE-2023-52809, CVE-2024-39495, CVE-2024-26651, CVE-2024-26880, CVE-2024-42228, CVE-2024-27437, CVE-2022-48863)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7028-1>

Solution

Update the affected kernel package.

Risk Factor

Critical

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

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-2021-47188
CVE	CVE-2022-48791
CVE	CVE-2022-48863
CVE	CVE-2023-52527
CVE	CVE-2023-52809
CVE	CVE-2024-26651
CVE	CVE-2024-26677
CVE	CVE-2024-26733
CVE	CVE-2024-26851

CVE	CVE-2024-26880
CVE	CVE-2024-26984
CVE	CVE-2024-27398
CVE	CVE-2024-27437
CVE	CVE-2024-38570
CVE	CVE-2024-38583
CVE	CVE-2024-39480
CVE	CVE-2024-39495
CVE	CVE-2024-40902
CVE	CVE-2024-42154
CVE	CVE-2024-42160
CVE	CVE-2024-42224
CVE	CVE-2024-42228
XREF	USN:7028-1

Plugin Information

Published: 2024/09/23, Modified: 2025/04/14

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-229-generic for this advisory.

132747 - Ubuntu 16.04 LTS / 18.04 LTS : NSS vulnerability (USN-4231-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4231-1 advisory.

It was discovered that NSS 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-4231-1>

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-2019-17006
XREF	USN:4231-1

Plugin Information

Published: 2020/01/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.10
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.10

126465 - Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4045-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4045-1 advisory.

A type confusion bug was discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could exploit this by causing a denial of service, or executing arbitrary code. (CVE-2019-11707)

It was discovered that a sandboxed child process could open arbitrary web content in the parent process via the Prompt:Open IPC message. When combined with another vulnerability, an attacker could potentially exploit this to execute arbitrary code. (CVE-2019-11708)

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-4045-1>

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

9.3 (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-2019-11707
CVE	CVE-2019-11708
XREF	USN:4045-1
XREF	CISA-KNOWN-EXPLOITED:2022/06/13
XREF	CEA-ID:CEA-2019-0458

Plugin Information

Published: 2019/07/03, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1

- Fixed package : thunderbird_1:60.7.2+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.7.2+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.7.2+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.7.2+build2-0ubuntu0.16.04.1

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 :

```
- sambashare - (readable)
+ Content of this share :
..
mailsent.txt
wordpress.bkp.zip
```

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: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

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 : less_481-2.1ubuntu0.2
- Fixed package : less_481-2.1ubuntu0.2+esm2

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 NFKC 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 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/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

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

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 : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm13
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm13
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm13
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm13
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm13

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 (CVSS:2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS:2#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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm23
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm23
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm23
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm23

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

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm12

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

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 : `klIBC-utils_2.0.4-8ubuntu1.16.04.4`
- Fixed package : `klIBC-utils_2.0.4-8ubuntu1.16.04.4+esm2`
- Installed package : `libklibc_2.0.4-8ubuntu1.16.04.4`
- Fixed package : `libklibc_2.0.4-8ubuntu1.16.04.4+esm2`

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/VC: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_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm3

232645 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : Jinja2 vulnerabilities (USN-7343-1)

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-7343-1 advisory.

Rafal Krupinski discovered that Jinja2 did not properly restrict the execution of code in situations where templates are used maliciously. An attacker with control over a template's filename and content could potentially use this issue to enable the execution of arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2024-56201)

It was discovered that Jinja2 sandboxed environments could be escaped through a call to a string format method. An attacker could possibly use this issue to enable the execution of arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2024-56326)

It was discovered that Jinja2 sandboxed environments could be escaped through the malicious use of certain filters. An attacker could possibly use this issue to enable the execution of arbitrary code.

(CVE-2025-27516)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7343-1>

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

High

CVSS v4.0 Base Score

5.4 (CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/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

6.8 (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-2024-56201
CVE	CVE-2024-56326
CVE	CVE-2025-27516
XREF	USN:7343-1

Plugin Information

Published: 2025/03/12, Modified: 2025/03/12

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-jinja2_2.8-1
- Fixed package : python3-jinja2_2.8-1ubuntu0.1+esm5

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/I: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: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

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 : krb5-locales_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2+esm6
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2+esm6
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2+esm6
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2+esm6
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2+esm6

216780 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libxml2 vulnerabilities (USN-7302-1)

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-7302-1 advisory.

It was discovered that libxml2 incorrectly handled certain memory operations. A remote attacker could use this issue to cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS. (CVE-2022-49043)

It was discovered that the libxml2 xmllint tool incorrectly handled certain memory operations. If a user or automated system were tricked into running xmllint on a specially crafted xml file, a remote attacker could cause xmllint to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS. (CVE-2024-34459)

It was discovered that libxml2 did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-56171)

It was discovered that libxml2 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-2025-24928)

It was discovered that libxml2 could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. (CVE-2025-27113)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7302-1>

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-2022-49043
CVE	CVE-2024-34459
CVE	CVE-2024-56171
CVE	CVE-2025-24928
CVE	CVE-2025-27113
XREF	IAVA:2024-A-0067-S
XREF	USN:7302-1
XREF	IAVA:2025-A-0123-S

Plugin Information

Published: 2025/02/25, Modified: 2025/04/10

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 : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm7

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

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 : krb5-locales_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2+esm5
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2+esm5
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2+esm5
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2+esm5
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2+esm5

211587 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-7015-5)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7015-5 advisory.

USN-7015-1 fixed several vulnerabilities in Python. This update provides the corresponding update for CVE-2024-6232 and CVE-2024-6923 for python2.7 in Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, 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-7015-5>

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-2024-6232
CVE	CVE-2024-6923
XREF	USN:7015-5

Plugin Information

Published: 2024/11/19, Modified: 2024/11/19

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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm12
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm12
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm12
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm12
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm12

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_1.1.28-2.1ubuntu0.1
- Fixed package : libxslt1.1_1.1.28-2.1ubuntu0.3+esm2

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm15

193082 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Bind vulnerabilities (USN-6723-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6723-1 advisory.

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6723-1>

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-2023-50387
CVE	CVE-2023-50868
XREF	USN:6723-1
XREF	IAVA:2024-A-0103-S

Plugin Information

Published: 2024/04/09, 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.

- Installed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm8

123751 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : BusyBox vulnerabilities (USN-3935-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3935-1 advisory.

Tyler Hicks discovered that BusyBox incorrectly handled symlinks inside tar archives. If a user or automated system were tricked into processing a specially crafted tar archive, a remote attacker could overwrite arbitrary files outside of the current directory. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2011-5325)

Mathias Krause discovered that BusyBox incorrectly handled kernel module loading restrictions. A local attacker could possibly use this issue to bypass intended restrictions. This issue only affected Ubuntu 14.04 LTS. (CVE-2014-9645)

It was discovered that BusyBox incorrectly handled certain ZIP archives. If a user or automated system were tricked into processing a specially crafted ZIP archive, a remote attacker could cause BusyBox to crash, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2015-9261)

Nico Golde discovered that the BusyBox DHCP client incorrectly handled certain malformed domain names. A remote attacker could possibly use this issue to cause the DHCP client to crash, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2016-2147)

Nico Golde discovered that the BusyBox DHCP client incorrectly handled certain 6RD options. A remote attacker could use this issue to cause the DHCP client to crash, leading to a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2016-2148)

It was discovered that BusyBox incorrectly handled certain bzip2 archives. If a user or automated system were tricked into processing a specially crafted bzip2 archive, a remote attacker could cause BusyBox to crash, leading to a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2017-15873)

It was discovered that BusyBox incorrectly handled tab completion. A local attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2017-16544)

It was discovered that the BusyBox wget utility incorrectly handled certain responses. A remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2018-1000517)

It was discovered that the BusyBox DHCP utilities incorrectly handled certain memory operations. A remote attacker could possibly use this issue to access sensitive information. (CVE-2018-20679, CVE-2019-5747)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3935-1>

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-2011-5325
CVE	CVE-2014-9645
CVE	CVE-2015-9261
CVE	CVE-2016-2147
CVE	CVE-2016-2148
CVE	CVE-2017-15873
CVE	CVE-2017-16544
CVE	CVE-2018-1000517
CVE	CVE-2018-20679
CVE	CVE-2019-5747
XREF	USN:3935-1

Plugin Information

Published: 2019/04/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : busybox-initramfs_1:1.22.0-15ubuntu1
- Fixed package : busybox-initramfs_1:1.22.0-15ubuntu1.4

- Installed package : busybox-static_1:1.22.0-15ubuntu1
- Fixed package : busybox-static_1:1.22.0-15ubuntu1.4

123502 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Firefox regression (USN-3918-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3918-3 advisory.

USN-3918-1 fixed vulnerabilities in Firefox. The update caused web compatibility issues with some websites. 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-3918-3>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:3918-3

Plugin Information

Published: 2019/03/29, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_66.0.2+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_66.0.2+build1-0ubuntu0.16.04.1

124114 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Firefox regressions (USN-3918-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3918-4 advisory.

USN-3918-1 fixed vulnerabilities in Firefox. The update caused web compatibility and performance issues with some websites. 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-3918-4>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:3918-4

Plugin Information

Published: 2019/04/17, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_66.0.3+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_66.0.3+build1-0ubuntu0.16.04.1

122533 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GD vulnerabilities (USN-3900-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3900-1 advisory.

It was discovered that GD incorrectly handled memory when processing certain images. A remote attacker could use this issue with a specially crafted image file to cause GD 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-3900-1>

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-2019-6977
CVE	CVE-2019-6978
XREF	USN:3900-1

Plugin Information

Published: 2019/03/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgd3_2.1.1-4ubuntu0.16.04.10
- Fixed package : libgd3_2.1.1-4ubuntu0.16.04.11

194950 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-6762-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6762-1 advisory.

It was discovered that GNU C Library incorrectly handled netgroup requests. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS.
(CVE-2014-9984)

It was discovered that GNU C Library might allow context-dependent attackers to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2015-20109)

It was discovered that GNU C Library when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution. This issue only affected Ubuntu 14.04 LTS.
(CVE-2018-11236)

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. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3999)

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. (CVE-2024-2961)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6762-1>

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-2014-9984
CVE	CVE-2015-20109
CVE	CVE-2018-11236
CVE	CVE-2021-3999
CVE	CVE-2024-2961
XREF	USN:6762-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/05/02, Modified: 2024/10/21

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm6
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm6
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm6
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm6
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm6
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm6

124085 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Libxslt vulnerability (USN-3947-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3947-1 advisory.

It was discovered that Libxslt incorrectly handled certain documents. An attacker could possibly use this issue to access 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-3947-1>

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-2019-11068
XREF	USN:3947-1

Plugin Information

Published: 2019/04/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libxslt1.1_1.1.28-2.1ubuntu0.1
- Fixed package : libxslt1.1_1.1.28-2.1ubuntu0.2

123505 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-3927-1)**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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3927-1 advisory.

It was discovered that Thunderbird allowed PAC files to specify that requests to localhost are sent through the proxy to another server. If proxy auto-detection is enabled, an attacker could potentially exploit this to conduct attacks on local services and tools. (CVE-2018-18506)

Multiple security issues were discovered in Thunderbird. If a user were tricked in to 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-2019-9788, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9795, CVE-2019-9796, CVE-2019-9810, CVE-2019-9813)

A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. If a user were tricked in to opening a specially crafted website in a browsing context with Spectre mitigations disabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2019-9793)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3927-1>

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

9.4 (CVSS:3.0/E:H/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

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

References

CVE	CVE-2018-18506
CVE	CVE-2019-9788
CVE	CVE-2019-9790
CVE	CVE-2019-9791
CVE	CVE-2019-9792
CVE	CVE-2019-9793
CVE	CVE-2019-9795
CVE	CVE-2019-9796
CVE	CVE-2019-9810
CVE	CVE-2019-9813
XREF	USN:3927-1

Plugin Information

Published: 2019/03/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:60.6.1+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.6.1+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.6.1+build2-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.6.1+build2-0ubuntu0.16.04.1

123973 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Wget vulnerabilities (USN-3943-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3943-1 advisory.

It was discovered that Wget incorrectly handled certain inputs. An attacker could possibly use this issue to access sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 18.10.

(CVE-2018-20483)

Kusano Kazuhiko discovered that Wget incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-5953)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3943-1>

Solution

Update the affected wget and / or wget-udeb 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-2018-20483
CVE	CVE-2019-5953
XREF	USN:3943-1

Plugin Information

Published: 2019/04/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : wget_1.17.1-1ubuntu1.4
- Fixed package : wget_1.17.1-1ubuntu1.5

206015 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6944-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6944-2 advisory.

USN-6944-1 fixed CVE-2024-7264 for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 24.04 LTS. This update provides the corresponding fix for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6944-2>

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:6944-2

Plugin Information

Published: 2024/08/21, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm13
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm13

214908 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libvpx vulnerability (USN-7249-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7249-1 advisory.

Xiantong Hou discovered that libvpx would overflow when attempting to allocate memory for very large images. If an application using libvpx opened a specially crafted file, a remote attacker could possibly use this issue to cause the application to crash, resulting in a denial of service, or the execution of 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-7249-1>

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
XREF

[CVE-2024-5197](#)

USN:7249-1

Plugin Information

Published: 2025/02/03, Modified: 2025/07/23

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.

- Installed package : libvpx3_1.5.0-2ubuntu1
- Fixed package : libvpx3_1.5.0-2ubuntu1.1+esm3

191794 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libxml2 vulnerability (USN-6658-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6658-2 advisory.

USN-6658-1 fixed a vulnerability in libxml2. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6658-2>

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

II

References

CVE	CVE-2024-25062
XREF	USN:6658-2
XREF	IAVA:2024-A-0067-S

Plugin Information

Published: 2024/03/11, Modified: 2025/02/21

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 : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm6

191736 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ncurses vulnerability (USN-6684-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6684-1 advisory.

It was discovered that ncurses incorrectly handled certain function return values, possibly leading to segmentation fault. 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-6684-1>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-50495
XREF	USN:6684-1

Plugin Information

Published: 2024/03/08, 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.

- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm5
- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm5
- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm5
- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm5
- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm5
- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm5

123679 - Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3931-2)

Synopsis

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

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3931-2 advisory.

USN-3931-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 LTS for Ubuntu 16.04 LTS and for the Linux Azure kernel for Ubuntu 14.04 LTS.

M. Vefa Bicakci and Andy Lutomirski discovered that the kernel did not properly set up all arguments to an error handler callback used when running as a paravirtualized guest. An unprivileged attacker in a paravirtualized guest VM could use this to cause a denial of service (guest VM crash). (CVE-2018-14678)

It was discovered that the KVM implementation in the Linux kernel on ARM 64bit processors did not properly handle some ioctls. An attacker with the privilege to create KVM-based virtual machines could use this to cause a denial of service (host system crash) or execute arbitrary code in the host. (CVE-2018-18021)

Mathias Payer and Hui Peng discovered a use-after-free vulnerability in the Advanced Linux Sound Architecture (ALSA) subsystem. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2018-19824)

Shlomi Oberman, Yuli Shapiro, and Ran Menscher discovered an information leak in the Bluetooth implementation of the Linux kernel. An attacker within Bluetooth range could use this to expose sensitive information (kernel memory). (CVE-2019-3459, CVE-2019-3460)

Jann Horn discovered that the KVM implementation in the Linux kernel contained a use-after-free vulnerability. An attacker in a guest VM with access to /dev/kvm could use this to cause a denial of service (guest VM crash). (CVE-2019-6974)

Jim Mattson and Felix Wilhelm discovered a use-after-free vulnerability in the KVM subsystem of the Linux kernel, when using nested virtual machines. A local attacker in a guest VM could use this to cause a denial of service (system crash) or possibly execute arbitrary code in the host system. (CVE-2019-7221)

Felix Wilhelm discovered that an information leak vulnerability existed in the KVM subsystem of the Linux kernel, when nested virtualization is used. A local attacker could use this to expose sensitive information (host system memory to a guest VM). (CVE-2019-7222)

Jann Horn discovered that the eBPF implementation in the Linux kernel was insufficiently hardened against Spectre V1 attacks. A local attacker could use this to expose sensitive information. (CVE-2019-7308)

It was discovered that a use-after-free vulnerability existed in the user-space API for crypto (af_alg) 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-2019-8912)

It was discovered that the Linux kernel did not properly deallocate memory when handling certain errors while reading files. A local attacker could use this to cause a denial of service (excessive memory consumption). (CVE-2019-8980)

Jann Horn discovered that the mmap implementation in the Linux kernel did not properly check for the mmap minimum address in some situations. A local attacker could use this to assist exploiting a kernel NULL pointer dereference vulnerability. (CVE-2019-9213)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3931-2>

Solution

Update the affected kernel package.

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

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2018-14678
CVE CVE-2018-18021
CVE CVE-2018-19824
CVE CVE-2019-3459
CVE CVE-2019-3460
CVE CVE-2019-6974
CVE CVE-2019-7221
CVE CVE-2019-7222
CVE CVE-2019-7308
CVE CVE-2019-8912
CVE CVE-2019-8980
CVE CVE-2019-9213
XREF USN:3931-2

Exploitable With

Metasploit (true)

Plugin Information

Published: 2019/04/03, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-47-generic for this advisory.

181766 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM : ImageMagick vulnerability (USN-6393-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6393-1 advisory.

It was discovered that ImageMagick did not properly handle memory when processing the -help option. An attacker could potentially 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-6393-1>

Solution

Update the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-48541
XREF	USN:6393-1
XREF	IAVB:2023-B-0065-S

Plugin Information

Published: 2023/09/21, 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.

- Installed package : `imagemagick_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick_8:6.8.9.9-7ubuntu5.16+esm9`
- Installed package : `imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm9`
- Installed package : `imagemagick-common_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm9`
- Installed package : `libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm9`
- Installed package : `libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm9`
- Installed package : `libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm9`

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: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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm20
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm20
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm20
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm20

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE-2022-33065
XREF USN:6471-1

Plugin Information

Published: 2023/11/03, 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.

- Installed package : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.3+esm3

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/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:L/Au:S/C: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

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_1.13.1-2ubuntu0.16.04.2
- Fixed package : python3-urllib3_1.13.1-2ubuntu0.16.04.4+esm1

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

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm5
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm5
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm5
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm5
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm5
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm5

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 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. (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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm12

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

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm5
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm5
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm5
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm8
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm8
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm8
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm5
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm5
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm8
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm8

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: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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm18
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm18
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm18
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm18

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm14

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

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 : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16+esm4
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16+esm4
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16+esm4

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

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_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm7`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm7`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm7`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm7`

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

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 : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16+esm3
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16+esm3
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16+esm3

186221 - Ubuntu 16.04 ESM / 18.04 ESM : Apache HTTP Server vulnerability (USN-6510-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6510-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6510-1>

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
XREF	USN:6510-1
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2023/11/23, 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.

- Installed package : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm11
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm11
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm11
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm11

178445 - Ubuntu 16.04 ESM / 18.04 ESM : Bind vulnerability (USN-6183-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6183-2 advisory.

USN-6183-1 fixed vulnerabilities in Bind. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6183-2>

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

STIG Severity

I

References

CVE	CVE-2023-2828
XREF	USN:6183-2
XREF	IAVA:2023-A-0320-S

Plugin Information

Published: 2023/07/18, Modified: 2024/10/29

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 : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm6

182789 - Ubuntu 16.04 ESM / 18.04 ESM : Bind vulnerability (USN-6421-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6421-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6421-1>

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/R:L/O:RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3341
XREF	USN:6421-1
XREF	IAVA:2023-A-0500-S

Plugin Information

Published: 2023/10/09, 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.

- Installed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm7

[183410 - Ubuntu 16.04 ESM / 18.04 ESM : GLib vulnerabilities \(USN-6165-2\)](#)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6165-2 advisory.

USN-6165-1 fixed vulnerabilities in GLib. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6165-2>

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-2023-29499
CVE	CVE-2023-32611
CVE	CVE-2023-32636
CVE	CVE-2023-32643
CVE	CVE-2023-32665
XREF	USN:6165-2

Plugin Information

Published: 2023/10/19, Modified: 2024/10/29

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 : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.8+esm3
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.8+esm3
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.8+esm3

178283 - Ubuntu 16.04 ESM / 18.04 ESM : LibTIFF vulnerabilities (USN-6229-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6229-1 advisory.

It was discovered that LibTIFF was not properly handling variables used to perform memory management operations when processing an image through tiffcrop, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.
(CVE-2023-25433, CVE-2023-26965)

It was discovered that LibTIFF was not properly processing numerical values when dealing with little-endian input data, which could lead to the execution of an invalid operation. An attacker could possibly use this issue to cause a denial of service (CVE-2023-26966)

It was discovered that LibTIFF was not properly performing bounds checks when closing a previously opened TIFF file, which could lead to a NULL pointer

dereference. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3316)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6229-1>

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-2023-3316
CVE	CVE-2023-25433
CVE	CVE-2023-26965
CVE	CVE-2023-26966
XREF	USN:6229-1

Plugin Information

Published: 2023/07/13, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm11

189608 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6604-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6604-1 advisory.

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)

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 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)

It was discovered that the CIFS network file system implementation in the Linux kernel did not properly validate the server frame size in certain situations, 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-6604-1>

Solution

Update the affected kernel package.

Risk Factor

High

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

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-2023-1079
CVE	CVE-2023-6606
CVE	CVE-2023-6931
CVE	CVE-2023-6932
CVE	CVE-2023-20588
CVE	CVE-2023-45863
XREF	USN:6604-1

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-221-generic for this advisory.

177901 - Ubuntu 16.04 ESM / 18.04 ESM : OpenLDAP vulnerability (USN-6197-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6197-1 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-6197-1>

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:6197-1

Plugin Information

Published: 2023/07/03, 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.

- Installed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13+esm2

183232 - Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerability (USN-6394-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6394-2 advisory.

USN-6394-1 fixed a vulnerability in Python. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6394-2>

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-2022-48560
XREF USN:6394-2

Plugin Information

Published: 2023/10/17, Modified: 2024/10/29

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm8
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm8
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm8
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm8
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm8

186844 - Ubuntu 16.04 ESM / 18.04 ESM : X.Org X Server vulnerabilities (USN-6555-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6555-2 advisory.

USN-6555-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6555-2>

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

7.8 (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:6555-2

Plugin Information

Published: 2023/12/14, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm8

177453 - Ubuntu 16.04 ESM / 18.04 ESM : libx11 vulnerability (USN-6168-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6168-2 advisory.

USN-6168-1 fixed a vulnerability in libx11. This update provides the corresponding update for Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6168-2>

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:6168-2

Plugin Information

Published: 2023/06/20, Modified: 2024/10/29

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 : libx11-6_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-6_2:1.6.3-1ubuntu2.2+esm2
- Installed package : libx11-data_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-data_2:1.6.3-1ubuntu2.2+esm2
- Installed package : libx11-xcb1_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-xcb1_2:1.6.3-1ubuntu2.2+esm2

183834 - Ubuntu 16.04 ESM / 18.04 ESM : ncurses vulnerability (USN-6451-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6451-1 advisory.

It was discovered that ncurses could be made to read out of bounds. 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-6451-1>

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/NC:H/Vl: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: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-2020-19189
XREF USN:6451-1

Plugin Information

Published: 2023/10/24, 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.

- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm4
- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm4
- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm4
- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm4
- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm4
- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm4

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 zero-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/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

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-2023-1579
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

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 : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm6

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

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm6
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm6
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm6
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm6

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

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 : dnsMasq-base_2.75-1ubuntu0.16.04.5
- Fixed package : dnsMasq-base_2.75-1ubuntu0.16.04.10+esm1

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

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 : dnsmasq-base_2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.79-1ubuntu0.16.04.1+esm2

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 [CVE-2022-43680](#)
XREF USN:5638-3

Plugin Information

Published: 2022/11/23, Modified: 2024/10/29

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 : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm7

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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20230214.0ubuntu0.16.04.1+esm1

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 tiffsplits. 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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm7

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

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 : liblouis-data_2.6.4-2ubuntu0.4
- Fixed package : liblouis-data_2.6.4-2ubuntu0.4+esm1
- Installed package : liblouis9_2.6.4-2ubuntu0.4
- Fixed package : liblouis9_2.6.4-2ubuntu0.4+esm1
- Installed package : python3-louis_2.6.4-2ubuntu0.4
- Fixed package : python3-louis_2.6.4-2ubuntu0.4+esm1

161809 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5443-1)

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-5443-1 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)

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-5443-1>

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-2022-29581
CVE	CVE-2022-30594
XREF	USN:5443-1

Plugin Information

Published: 2022/06/03, Modified: 2024/08/29

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-180-generic for this advisory.

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
XREF-USN:5625-1

Plugin Information

Published: 2022/09/21, 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.

- Installed package : python3-mako_1.0.3+ds1-1ubuntu1
- Fixed package : python3-mako_1.0.3+ds1-1ubuntu1+esm1

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

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm2
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm2
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm2
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm3
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm3
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm3
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm2
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm2
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm3
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm3

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

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm4
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm4
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm4
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm7
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm7
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm7
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm4
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm4
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm7
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm7

173039 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-5963-1)

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-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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm17

- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm17

- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm17

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm17
```

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

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm4
```

- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm3
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm3

174458 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : libxml2 vulnerabilities (USN-6028-1)

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-6028-1 advisory.

It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2023-28484)

It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash. (CVE-2023-29469)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6028-1>

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-2023-28484
CVE	CVE-2023-29469
XREF	USN:6028-1

Plugin Information

Published: 2023/04/19, 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.

- Installed package : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm5

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

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 : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16+esm1
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16+esm1
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16+esm1

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/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

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-2019-18276
XREF	USN:5380-1

Plugin Information

Published: 2022/04/20, 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.

- Installed package : bash_4.3-14ubuntu1.2
- Fixed package : bash_4.3-14ubuntu1.4+esm1

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

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 : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm2

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

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 : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm5

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

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 : gstreamer1.0-plugins-good_1.8.3-1ubuntu0.4
- Fixed package : gstreamer1.0-plugins-good_1.8.3-1ubuntu0.5+esm1
- Installed package : gstreamer1.0-pulseaudio_1.8.3-1ubuntu0.4
- Fixed package : gstreamer1.0-pulseaudio_1.8.3-1ubuntu0.5+esm1
- Installed package : libgstreamer-plugins-good1.0-0_1.8.3-1ubuntu0.4
- Fixed package : libgstreamer-plugins-good1.0-0_1.8.3-1ubuntu0.5+esm1

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

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 : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

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	CVE-2022-41916
XREF	USN:5766-1

Plugin Information

Published: 2022/12/08, 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.

- Installed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

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 NFS 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-202-generic for this advisory.

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 handled 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 klibc 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 klibc 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 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

8.5 (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

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 : klibc-utils_2.0.4-8ubuntu1.16.04.4
- Fixed package : klibc-utils_2.0.4-8ubuntu1.16.04.4+esm1
- Installed package : libklibc_2.0.4-8ubuntu1.16.04.4
- Fixed package : libklibc_2.0.4-8ubuntu1.16.04.4+esm1

150858 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libxml2 vulnerabilities (USN-4991-1)

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-4991-1 advisory.

Yunho Kim discovered that libxml2 incorrectly handled certain error conditions. A remote attacker could exploit this with a crafted XML file to cause a denial of service, or possibly cause libxml2 to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, and Ubuntu 16.04 ESM. (CVE-2017-8872)

Zhipeng Xie discovered that libxml2 incorrectly handled certain XML schemas. A remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. (CVE-2019-20388)

It was discovered that libxml2 incorrectly handled invalid UTF-8 input. A remote attacker could possibly exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2020-24977)

It was discovered that libxml2 incorrectly handled invalid UTF-8 input. A remote attacker could possibly exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service.
(CVE-2021-3517)

It was discovered that libxml2 did not properly handle certain crafted XML files. A local attacker could exploit this with a crafted input to cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-3516, CVE-2021-3518)

It was discovered that libxml2 incorrectly handled error states. A remote attacker could exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. (CVE-2021-3537)

Sebastian Pipping discovered that libxml2 did not properly handle certain crafted XML files. A remote attacker could exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. (CVE-2021-3541)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4991-1>

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

8.2 (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-2017-8872
CVE	CVE-2019-20388
CVE	CVE-2020-24977
CVE	CVE-2021-3516
CVE	CVE-2021-3517
CVE	CVE-2021-3518
CVE	CVE-2021-3537
CVE	CVE-2021-3541
XREF	USN:4991-1

Plugin Information

Published: 2021/06/17, 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.

- Installed package : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm1

162515 - Ubuntu 16.04 ESM / 18.04 LTS : Apache HTTP Server regression (USN-5487-3)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5487-3 advisory.

USN-5487-1 fixed several vulnerabilities in Apache HTTP Server. Unfortunately it caused regressions.

USN-5487-2 reverted the patches that caused the regression in Ubuntu 14.04 ESM for further investigation.

This update re-adds the security fixes for Ubuntu 14.04 ESM and fixes two different regressions: one affecting mod_proxy only in Ubuntu 14.04 ESM and another in mod_sed affecting also Ubuntu 16.04 ESM and 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5487-3>

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

8.5 (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:5487-3
XREF IAVA:2022-A-0230-S

Plugin Information

Published: 2022/06/23, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm7
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm7
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm7
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm7

149410 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4946-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4946-1 advisory.

It was discovered that the DRM subsystem in the Linux kernel contained double-free vulnerabilities. A privileged attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-20292)

Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H. Schuherr 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)

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 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 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 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-4946-1>

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-2021-20292
CVE	CVE-2021-26930
CVE	CVE-2021-26931
CVE	CVE-2021-28038
CVE	CVE-2021-28688
CVE	CVE-2021-29264
CVE	CVE-2021-29265
CVE	CVE-2021-29650
CVE	CVE-2021-30002
XREF	USN:4946-1

Plugin Information

Published: 2021/05/12, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-143-generic for this advisory.

150155 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4979-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4979-1 advisory.

Kiycin () 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)

Kiycin () 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)

Kiycin () 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 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)

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 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)

It was discovered that the CIPSO implementation in the Linux kernel did not properly perform reference counting in some situations, leading to use-after-free vulnerabilities. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33033)

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)

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-4979-1>

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-2020-25670
CVE	CVE-2020-25671
CVE	CVE-2020-25672
CVE	CVE-2020-25673
CVE	CVE-2021-3428
CVE	CVE-2021-3483
CVE	CVE-2021-28660
CVE	CVE-2021-28964
CVE	CVE-2021-28971
CVE	CVE-2021-28972
CVE	CVE-2021-29647
CVE	CVE-2021-31916
CVE	CVE-2021-33033
XREF	USN:4979-1

Plugin Information

Published: 2021/06/03, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-144-generic for this advisory.

151920 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5018-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5018-1 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)

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 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 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)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5018-1>

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/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2020-24586
CVE	CVE-2020-24587
CVE	CVE-2020-26139
CVE	CVE-2020-26147
CVE	CVE-2020-26558
CVE	CVE-2021-0129
CVE	CVE-2021-23134
CVE	CVE-2021-31829
CVE	CVE-2021-32399
CVE	CVE-2021-33034
CVE	CVE-2021-33200
CVE	CVE-2021-33909
XREF	USN:5018-1
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/21, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-151-generic for this advisory.

153177 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5073-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5073-1 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)

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)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5073-1>

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-2021-3612
CVE	CVE-2021-3653
CVE	CVE-2021-3656
CVE	CVE-2021-34693
CVE	CVE-2021-38160
XREF	USN:5073-1

Plugin Information

Published: 2021/09/09, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-156-generic for this advisory.

153797 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5094-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5094-1 advisory.

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)

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)

Alois Wohlschläger 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)

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 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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5094-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v4.0 Base Score

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

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-2021-3732
CVE	CVE-2021-22543
CVE	CVE-2021-37576
CVE	CVE-2021-38204
CVE	CVE-2021-38205
XREF	USN:5094-1

Plugin Information

Published: 2021/09/30, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-159-generic for this advisory.

156484 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5209-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5209-1 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 a race condition existed in the timer implementation in the Linux kernel. A privileged attacker could use this to cause a denial of service. (CVE-2021-20317)

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 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-5209-1>

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-2021-3760
CVE	CVE-2021-4002
CVE	CVE-2021-20317
CVE	CVE-2021-20321
CVE	CVE-2021-41864
CVE	CVE-2021-43389
XREF	USN:5209-1

Plugin Information

Published: 2022/01/06, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-166-generic for this advisory.

157352 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5268-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5268-1 advisory.

Keyu Man discovered that the ICMP implementation in the Linux kernel did not properly handle received ICMP error packets. A remote attacker could use this to facilitate attacks on UDP based services that depend on source port randomization. (CVE-2021-20322)

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-5268-1>

Solution

Update the affected kernel 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: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

7.9 (CVSS2#AV:A/AC:M/Au:N/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-2021-20322
CVE	CVE-2021-42739
XREF	USN:5268-1

Plugin Information

Published: 2022/02/03, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-167-generic for this advisory.

158249 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5298-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5298-1 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)

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)

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)

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-5298-1>

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-2021-4083
CVE	CVE-2021-4155
CVE	CVE-2021-4202
CVE	CVE-2021-22600
CVE	CVE-2021-28711
CVE	CVE-2021-28712
CVE	CVE-2021-28713
CVE	CVE-2021-28714
CVE	CVE-2021-28715
CVE	CVE-2021-39685
CVE	CVE-2022-0330
CVE	CVE-2022-22942
XREF	USN:5298-1
XREF	CISA-KNOWN-EXPLOITED:2022/05/02

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/02/22, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-169-generic for this advisory.

159143 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5339-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5339-1 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)

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)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5339-1>

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-2021-3506
CVE	CVE-2021-43976
CVE	CVE-2021-44733
CVE	CVE-2021-45095
CVE	CVE-2022-0435
CVE	CVE-2022-0492
XREF	USN:5339-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/03/22, Modified: 2024/08/29

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-173-generic for this advisory.

163111 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5515-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5515-1 advisory.

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)

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)

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)

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)

Zheyu Ma discovered that the Silicon Motion SM712 framebuffer driver in the Linux kernel did not properly handle very small reads. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-2380)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5515-1>

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-2021-4197
CVE	CVE-2022-1011
CVE	CVE-2022-1198
CVE	CVE-2022-1199
CVE	CVE-2022-1204
CVE	CVE-2022-1205
CVE	CVE-2022-1353
CVE	CVE-2022-1516
CVE	CVE-2022-2380
CVE	CVE-2022-28389
XREF	USN:5515-1

Plugin Information

Published: 2022/07/14, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-189-generic for this advisory.

176458 - Ubuntu 16.04 ESM / 18.04 LTS : Perl vulnerability (USN-6112-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6112-1 advisory.

It was discovered that Perl was not properly verifying TLS certificates when using CPAN together with HTTP::Tiny to download modules over HTTPS. If a remote attacker were able to intercept communications, this flaw could potentially be used to install altered modules.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6112-1>

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

7.3 (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:6112-1

Plugin Information

Published: 2023/05/29, 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.

- Installed package : libperl5.22_5.22.1-9ubuntu0.6
- Fixed package : libperl5.22_5.22.1-9ubuntu0.9+esm2
- Installed package : perl_5.22.1-9ubuntu0.6
- Fixed package : perl_5.22.1-9ubuntu0.9+esm2
- Installed package : perl-base_5.22.1-9ubuntu0.6
- Fixed package : perl-base_5.22.1-9ubuntu0.9+esm2
- Installed package : perl-modules-5.22_5.22.1-9ubuntu0.6
- Fixed package : perl-modules-5.22_5.22.1-9ubuntu0.9+esm2

157160 - Ubuntu 16.04 ESM / 18.04 LTS : shadow vulnerabilities (USN-5254-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5254-1 advisory.

It was discovered that shadow incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or expose sensitive information. This issue only affected Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. (CVE-2017-12424)

It was discovered that shadow incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. (CVE-2018-7169)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5254-1>

Solution

Update the affected login, passwd and / or uidmap 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-2017-12424
CVE	CVE-2018-7169
XREF	USN:5254-1

Plugin Information

Published: 2022/01/27, 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.

- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm1

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm1

150942 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerabilities (USN-4994-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4994-2 advisory.

USN-4994-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4994-2>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-35452
CVE	CVE-2021-26690
CVE	CVE-2021-26691
CVE	CVE-2021-30641
XREF	USN:4994-2
XREF	IAVA:2021-A-0259-S

Plugin Information

Published: 2021/06/21, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm1
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm1
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm1
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm1

153766 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerabilities (USN-5090-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5090-2 advisory.

USN-5090-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5090-2>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
CVE	CVE-2021-40438
XREF	USN:5090-2
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/09/27, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm2
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm2
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm2
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm2

156568 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerabilities (USN-5212-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5212-2 advisory.

USN-5212-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5212-2>

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-2021-44224
CVE	CVE-2021-44790
XREF	USN:5212-2
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2022/01/10, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm4
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm4
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm4
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm4

[159058 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerabilities \(USN-5333-2\)](#)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5333-2 advisory.

USN-5333-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5333-2>

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

8.5 (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:5333-2
XREF	IAVA:2022-A-0124-S

Plugin Information

Published: 2022/03/18, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm5
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm5
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm5
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm5

170912 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerabilities (USN-5834-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5834-1 advisory.

It was discovered that the Apache HTTP Server mod_dav module did not properly handle specially crafted request headers. A remote attacker could possibly use this issue to cause the process to crash, leading to a denial of service. (CVE-2006-20001)

It was discovered that the Apache HTTP Server mod_proxy_ajp module did not properly handle certain invalid Transfer-Encoding headers. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2022-36760)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5834-1>

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
XREF	USN:5834-1
XREF	IAVA:2023-A-0047-S

Plugin Information

Published: 2023/01/31, 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.

- Installed package : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm8
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm8
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm8
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm8

165289 - Ubuntu 16.04 ESM : Bind vulnerabilities (USN-5626-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5626-2 advisory.

USN-5626-1 fixed several vulnerabilities in Bind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5626-2>

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/V:I:N/VA:L/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2795
CVE	CVE-2022-38177
XREF	USN:5626-2

Plugin Information

Published: 2022/09/21, Modified: 2024/10/29

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 : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm3

150846 - Ubuntu 16.04 ESM : BlueZ vulnerabilities (USN-4989-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4989-2 advisory.

USN-4989-1 fixed several vulnerabilities in BlueZ. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4989-2>

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:O/RC:C)

References

CVE CVE-2020-26558
CVE CVE-2020-27153
XREF USN:4989-2

Plugin Information

Published: 2021/06/17, Modified: 2024/10/29

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 : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3+esm1
- Installed package : bluez-cups_5.37-0ubuntu5.1
- Fixed package : bluez-cups_5.37-0ubuntu5.3+esm1
- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3+esm1
- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3+esm1

161728 - Ubuntu 16.04 ESM : CUPS vulnerabilities (USN-5454-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5454-2 advisory.

USN-5454-1 fixed several vulnerabilities in CUPS. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5454-2>

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:5454-2

Plugin Information

Published: 2022/06/01, Modified: 2024/10/29

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm1
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm1
- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.11+esm1
- Installed package : libcurlcgi1_2.1.3-4ubuntu0.7
- Fixed package : libcurlcgi1_2.1.3-4ubuntu0.11+esm1
- Installed package : libcurlimage2_2.1.3-4ubuntu0.7
- Fixed package : libcurlimage2_2.1.3-4ubuntu0.11+esm1
- Installed package : libcurlsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsmime1_2.1.3-4ubuntu0.11+esm1
- Installed package : libcurlsppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsppdc1_2.1.3-4ubuntu0.11+esm1

183695 - Ubuntu 16.04 ESM : DBD::mysql vulnerabilities (USN-5344-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5344-1 advisory.

It was discovered that the DBD::mysql module, when configured with server-side prepared statement support, was susceptible to operations that would result in improper memory access. An attacker could possibly use this issue to cause DBD::mysql to crash, resulting in a denial of service. (CVE-2016-1249, CVE-2016-1251)

It was discovered that the DBD::mysql module was susceptible to an operation that would result in improper memory access, introduced through incorrect documentation and code examples. An attacker could possibly use this issue to cause DBD::mysql to crash or potentially cause other, unspecified, impact. (CVE-2017-10788)

It was discovered that the DBD::mysql module processed SSL/TLS settings in a way that did not fully correlate with the respective documentation for each setting. An attacker could possibly use this to perform a cleartext-downgrade attack. (CVE-2017-10789)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5344-1>

Solution

Update the affected libdbd-mysql-perl 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-2016-1249
CVE	CVE-2016-1251
CVE	CVE-2017-10788
CVE	CVE-2017-10789
XREF	USN:5344-1

Plugin Information

Published: 2023/10/23, 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.

- Installed package : libdbd-mysql-perl_4.033-1ubuntu0.1
- Fixed package : libdbd-mysql-perl_4.033-1ubuntu0.1+esm1

156914 - Ubuntu 16.04 ESM : DBus vulnerability (USN-5244-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5244-1 advisory.

Daniel Onaca discovered that DBus contained a use-after-free vulnerability, caused by the incorrect handling of usernames sharing the same UID. An attacker could possibly use this issue to cause DBus 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-5244-1>

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE
XREF

CVE-2020-35512
USN:5244-1

Plugin Information

Published: 2022/01/20, 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.

- Installed package : dbus_1.10.6-1ubuntu3.3
- Fixed package : dbus_1.10.6-1ubuntu3.6+esm1
- Installed package : dbus-x11_1.10.6-1ubuntu3.3
- Fixed package : dbus-x11_1.10.6-1ubuntu3.6+esm1
- Installed package : libdbus-1-3_1.10.6-1ubuntu3.3
- Fixed package : libdbus-1-3_1.10.6-1ubuntu3.6+esm1

165463 - Ubuntu 16.04 ESM : Expat vulnerability (USN-5638-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5638-1 advisory.

Rhodri James discovered that Expat incorrectly handled memory when processing certain malformed XML 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-5638-1>

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-40674
XREF	USN:5638-1

Plugin Information

Published: 2022/09/26, 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.

- Installed package : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm6

172131 - Ubuntu 16.04 ESM : FriBidi vulnerabilities (USN-5922-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5922-1 advisory.

It was discovered that FriBidi incorrectly handled the processing of input strings, resulting in memory corruption. An attacker could possibly 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 possibly 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. An attacker could possibly 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-5922-1>

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:5922-1

Plugin Information

Published: 2023/03/06, 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.

- Installed package : libfribidi0_0.19.7-1
- Fixed package : libfribidi0_0.19.7-1ubuntu0.1~esm1

158680 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5310-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5310-2 advisory.

USN-5310-1 fixed several vulnerabilities in GNU. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5310-2>

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-2021-3999
CVE	CVE-2022-23218
CVE	CVE-2022-23219
XREF	USN:5310-2

Plugin Information

Published: 2022/03/07, Modified: 2024/10/29

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm1
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm1
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm1
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm1
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm1
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm1

151919 - Ubuntu 16.04 ESM : GNU binutils vulnerabilities (USN-4336-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4336-2 advisory.

USN-4336-1 fixed several vulnerabilities in GNU binutils. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4336-2>

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-2016-2226
CVE-2016-4487
CVE-2016-4488
CVE-2016-4489
CVE-2016-4490
CVE-2016-4491
CVE-2016-4492
CVE-2016-4493
CVE-2016-6131
CVE-2017-6965
CVE-2017-6966
CVE-2017-6969
CVE-2017-7209
CVE-2017-7210
CVE-2017-7223
CVE-2017-7224
CVE-2017-7225
CVE-2017-7226
CVE-2017-7227
CVE-2017-7299
CVE-2017-7300
CVE-2017-7301
CVE-2017-7302
CVE-2017-7614
CVE-2017-8393
CVE-2017-8394
CVE-2017-8395
CVE-2017-8396
CVE-2017-8397
CVE-2017-8398
CVE-2017-8421
CVE-2017-9038
CVE-2017-9039
CVE-2017-9040
CVE-2017-9041
CVE-2017-9042
CVE-2017-9044
CVE-2017-9742
CVE-2017-9744
CVE-2017-9745
CVE-2017-9746
CVE-2017-9747
CVE-2017-9748
CVE-2017-9749
CVE-2017-9750
CVE-2017-9751
CVE-2017-9752
CVE-2017-9753
CVE-2017-9754
CVE-2017-9755
CVE-2017-9756
CVE-2017-9954
CVE-2017-12448
CVE-2017-12449
CVE-2017-12450
CVE-2017-12451
CVE-2017-12452
CVE-2017-12453
CVE-2017-12454
CVE-2017-12455
CVE-2017-12456
CVE-2017-12457
CVE-2017-12458
CVE-2017-12459
CVE-2017-12799
CVE-2017-12967
CVE-2017-13710
CVE-2017-14128
CVE-2017-14129
CVE-2017-14130
CVE-2017-14333
CVE-2017-14529
CVE-2017-14930

CVE-CVE-2017-14932
CVE-CVE-2017-14938
CVE-CVE-2017-14939
CVE-CVE-2017-14940
CVE-CVE-2017-15020
CVE-CVE-2017-15021
CVE-CVE-2017-15022
CVE-CVE-2017-15024
CVE-CVE-2017-15025
CVE-CVE-2017-15225
CVE-CVE-2017-15938
CVE-CVE-2017-15939
CVE-CVE-2017-15996
CVE-CVE-2017-16826
CVE-CVE-2017-16827
CVE-CVE-2017-16828
CVE-CVE-2017-16831
CVE-CVE-2017-16832
CVE-CVE-2017-17080
CVE-CVE-2017-17121
CVE-CVE-2017-17123
CVE-CVE-2017-17124
CVE-CVE-2017-17125
CVE-CVE-2018-6323
CVE-CVE-2018-6543
CVE-CVE-2018-6759
CVE-CVE-2018-7208
CVE-CVE-2018-7568
CVE-CVE-2018-7569
CVE-CVE-2018-7642
CVE-CVE-2018-7643
CVE-CVE-2018-8945
CVE-CVE-2018-9138
CVE-CVE-2018-10372
CVE-CVE-2018-10373
CVE-CVE-2018-10534
CVE-CVE-2018-10535
CVE-CVE-2018-12641
CVE-CVE-2018-12697
CVE-CVE-2018-12698
CVE-CVE-2018-12699
CVE-CVE-2018-12934
CVE-CVE-2018-13033
CVE-CVE-2018-17358
CVE-CVE-2018-17359
CVE-CVE-2018-17360
CVE-CVE-2018-17794
CVE-CVE-2018-17985
CVE-CVE-2018-18309
CVE-CVE-2018-18483
CVE-CVE-2018-18484
CVE-CVE-2018-18605
CVE-CVE-2018-18606
CVE-CVE-2018-18607
CVE-CVE-2018-18700
CVE-CVE-2018-18701
CVE-CVE-2018-19931
CVE-CVE-2018-19932
CVE-CVE-2018-20002
CVE-CVE-2018-20623
CVE-CVE-2018-20671
CVE-CVE-2018-1000876
CVE-CVE-2019-9070
CVE-CVE-2019-9071
CVE-CVE-2019-9073
CVE-CVE-2019-9074
CVE-CVE-2019-9075
CVE-CVE-2019-9077
CVE-CVE-2019-12972
CVE-CVE-2019-14250
CVE-CVE-2019-14444
CVE-CVE-2019-17450
CVE-CVE-2019-17451
XREF-USN:4336-2

Plugin Information

Published: 2021/07/21, Modified: 2024/10/29

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 : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm1

157349 - Ubuntu 16.04 ESM : GPT fdisk vulnerabilities (USN-5262-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5262-1 advisory.

The potential for an out of bounds write due to a missing bounds check was discovered to impact the sgdisk utility of GPT fdisk.

Exploitation requires the use of a maliciously formatted storage

device and could cause sgdisk to crash as well as possibly

allow for local privilege escalation.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5262-1>

Solution

Update the affected gdisk package.

Risk Factor

High

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

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-2020-0256
CVE	CVE-2021-0308
XREF	USN:5262-1

Plugin Information

Published: 2022/02/03, 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.

- Installed package : gdisk_1.0.1-1build1
- Fixed package : gdisk_1.0.1-1ubuntu0.1~esm2

159725 - Ubuntu 16.04 ESM : Gzip vulnerability (USN-5378-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5378-4 advisory.

USN-5378-1 fixed a vulnerability in Gzip. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5378-4>

Solution

Update the affected gzip package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-1271
XREF	USN:5378-4
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/13, Modified: 2024/10/29

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 : gzip_1.6-4ubuntu1
- Fixed package : gzip_1.6-4ubuntu1+esm1

174409 - Ubuntu 16.04 ESM : ImageMagick vulnerabilities (USN-5855-4)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5855-4 advisory.

USN-5855-1 fixed vulnerabilities in ImageMagick. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5855-4>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-44267
CVE	CVE-2022-44268
XREF	USN:5855-4
XREF	IAVB:2023-B-0006-S

Plugin Information

Published: 2023/04/17, Modified: 2024/10/29

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 : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm7
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm7
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm7
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm7
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm7
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm7

150712 - Ubuntu 16.04 ESM : LZ4 vulnerability (USN-4968-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-4968-2 advisory.

USN-4968-1 fixed a vulnerability in LZ4. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4968-2>

Solution

Update the affected liblz4-1, liblz4-dev and / or liblz4-tool 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:4968-2

Plugin Information

Published: 2021/06/11, Modified: 2024/10/29

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 : liblz4-1_0.0~r131-2ubuntu2
- Fixed package : liblz4-1_0.0~r131-2ubuntu2+esm1

166669 - Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5705-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5705-1 advisory.

Chintan Shah discovered that LibTIFF incorrectly handled memory in certain conditions. 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. (CVE-2022-3570)

It was discovered that LibTIFF incorrectly handled memory in certain conditions. An attacker could trick a user into processing a specially crafted tiff file and potentially use this issue to cause a denial of service. (CVE-2022-3598)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5705-1>

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-2022-3570
CVE	CVE-2022-3598
XREF	USN:5705-1

Plugin Information

Published: 2022/10/28, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm6

159328 - Ubuntu 16.04 ESM : Libasn1 vulnerability (USN-5352-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5352-1 advisory.

It was discovered that Libasn1 incorrectly handled certain 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-5352-1>

Solution

Update the affected packages.

Risk Factor

High

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

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-2018-1000654
XREF USN:5352-1

Plugin Information

Published: 2022/03/30, 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.

- Installed package : libtasn1-6_4.7-3ubuntu0.16.04.3
- Fixed package : libtasn1-6_4.7-3ubuntu0.16.04.3+esm2

166748 - Ubuntu 16.04 ESM : Libtasn1 vulnerability (USN-5707-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5707-1 advisory.

It was discovered that Libtasn1 did not properly perform bounds checking. 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-5707-1>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-46848
XREF	USN:5707-1

Plugin Information

Published: 2022/10/31, 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.

- Installed package : libtasn1-6_4.7-3ubuntu0.16.04.3
- Fixed package : libtasn1-6_4.7-3ubuntu0.16.04.3+esm3

164016 - Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5560-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5560-2 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)

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)

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)

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 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)

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)

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-5560-2>

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

7.5 (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-2022-0494
CVE	CVE-2022-1048
CVE	CVE-2022-1195
CVE	CVE-2022-1652
CVE	CVE-2022-1679
CVE	CVE-2022-1729
CVE	CVE-2022-1734
CVE	CVE-2022-1974
CVE	CVE-2022-1975
CVE	CVE-2022-2586
CVE	CVE-2022-2588
CVE	CVE-2022-33981
CVE	CVE-2022-34918
XREF	USN:5560-2
XREF	CISA-KNOWN-EXPLOITED:2024/07/17

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2022/08/10, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-191-generic for this advisory.

173618 - Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5981-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5981-1 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 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)

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 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)

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)

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)

Wei Chen discovered that the DVB USB AZ6027 driver in the Linux kernel contained a null pointer dereference when handling certain messages from user space. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-28328)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5981-1>

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-2021-3669
CVE	CVE-2022-3424
CVE	CVE-2022-36280
CVE	CVE-2022-41218

CVE	CVE-2022-47929
CVE	CVE-2023-0045
CVE	CVE-2023-0266
CVE	CVE-2023-0394
CVE	CVE-2023-23455
CVE	CVE-2023-23559
CVE	CVE-2023-28328
XREF	USN:5981-1
XREF	CISA-KNOWN-EXPLOITED:2023/04/20

Plugin Information

Published: 2023/03/28, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-208-generic for this advisory.

164538 - Ubuntu 16.04 ESM : Linux kernel vulnerability (USN-5591-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5591-1 advisory.

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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5591-1>

Solution

Update the affected kernel package.

Risk Factor

High

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

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-2021-33656
XREF	USN:5591-1

Plugin Information

Published: 2022/08/31, Modified: 2024/08/29

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-192-generic for this advisory.

175288 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-6060-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6060-2 advisory.

USN-6060-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6060-2>

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-2023-21912
CVE	CVE-2023-21980
XREF	USN:6060-2

Plugin Information

Published: 2023/05/08, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.42-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.42-0ubuntu0.16.04.1+esm1

155923 - Ubuntu 16.04 ESM : NSS regression (USN-5168-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5168-4 advisory.

USN-5168-3 fixed a vulnerability in NSS. Unfortunately that update introduced a regression that could break SSL connections. 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-5168-4>

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:5168-4

Plugin Information

Published: 2021/12/08, Modified: 2024/10/29

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 : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.14+esm2
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.14+esm2

155767 - Ubuntu 16.04 ESM : NSS vulnerability (USN-5168-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5168-3 advisory.

USN-5168-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5168-3>

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-2021-43527
XREF USN:5168-3

Plugin Information

Published: 2021/12/02, Modified: 2024/10/29

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 : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.14+esm1
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.14+esm1

163755 - Ubuntu 16.04 ESM : NTFS-3G vulnerabilities (USN-5463-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5463-2 advisory.

USN-5463-1 fixed vulnerabilities in NTFS-3G. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5463-2>

Solution

Update the affected ntfs-3g and / or ntfs-3g-dev 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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

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:5463-2

Plugin Information

Published: 2022/08/03, Modified: 2024/10/29

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 : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.3+esm3

170082 - Ubuntu 16.04 ESM : Net-SNMP vulnerabilities (USN-5795-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5795-2 advisory.

USN-5795-1 and 5543-1 fixed several vulnerabilities in Net-SNMP. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5795-2>

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

7.9 (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)

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
CVE	CVE-2022-44792
CVE	CVE-2022-44793
XREF	USN:5795-2
XREF	IAVA:2022-A-0305

Plugin Information

Published: 2023/01/16, Modified: 2025/02/11

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 : libsnmp-base_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp-base_5.7.3+dfsg-1ubuntu4.6+esm1
- Installed package : libsnmp30_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp30_5.7.3+dfsg-1ubuntu4.6+esm1

161386 - Ubuntu 16.04 ESM : OpenLDAP vulnerability (USN-5424-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5424-2 advisory.

USN-5424-1 fixed a vulnerability in OpenLDAP. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5424-2>

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-2022-29155
XREF	USN:5424-2

Plugin Information

Published: 2022/05/19, Modified: 2024/10/29

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 : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13+esm1

171109 - Ubuntu 16.04 ESM : OpenSSL vulnerabilities (USN-5845-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5845-2 advisory.

USN-5845-1 fixed several vulnerabilities in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5845-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:H/I:H/V:A:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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-2023-0215
CVE	CVE-2023-0286
XREF	USN:5845-2

Plugin Information

Published: 2023/02/07, 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.

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0_0_1.0.2g-1ubuntu4.20+esm6
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm6

177537 - Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-6188-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6188-1 advisory.

Matt Caswell discovered that OpenSSL incorrectly handled certain ASN.1 object identifiers. A remote attacker could possibly use this issue to cause OpenSSL 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-6188-1>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:H/I:H/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:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2650
XREF	USN:6188-1
XREF	IAVA:2023-A-0158-S

Plugin Information

Published: 2023/06/22, 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.

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm9

- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm9

156772 - Ubuntu 16.04 ESM : Pillow vulnerabilities (USN-5227-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5227-2 advisory.

USN-5227-1 fixed several vulnerabilities in Pillow. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5227-2>

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-2021-23437
CVE	CVE-2021-34552
CVE	CVE-2022-22815
CVE	CVE-2022-22816
CVE	CVE-2022-22817
XREF	USN:5227-2

Plugin Information

Published: 2022/01/17, Modified: 2024/10/29

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-pil_3.1.2-0ubuntu1.1
- Fixed package : python3-pil_3.1.2-0ubuntu1.6+esm1

157085 - Ubuntu 16.04 ESM : PolicyKit vulnerability (USN-5252-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5252-2 advisory.

USN-5252-1 fixed a vulnerability in policykit-1. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5252-2>

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

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

I

References

CVE	CVE-2021-4034
XREF	USN:5252-2
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: 2024/10/29

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 : libpolkit-agent-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-agent-1-0_0.105-14.1ubuntu0.5+esm1
- Installed package : libpolkit-backend-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-backend-1-0_0.105-14.1ubuntu0.5+esm1
- Installed package : libpolkit-gobject-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-gobject-1-0_0.105-14.1ubuntu0.5+esm1
- Installed package : policykit-1_0.105-14.1ubuntu0.4
- Fixed package : policykit-1_0.105-14.1ubuntu0.5+esm1

153448 - Ubuntu 16.04 ESM : Python vulnerabilities (USN-5083-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5083-1 advisory.

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 16.04 ESM. (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. (CVE-2021-3737)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5083-1>

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)

STIG Severity

|

References

CVE	CVE-2021-3733
CVE	CVE-2021-3737
XREF	USN:5083-1
XREF	IAVA:2021-A-0497-S

Plugin Information

Published: 2021/09/16, 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.

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm1
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm1
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm1
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm1
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm1

165319 - Ubuntu 16.04 ESM : Python vulnerability (USN-5629-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5629-1 advisory.

It was discovered that the Python http.server module incorrectly handled certain URIs. An attacker could potentially use this to redirect web traffic.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5629-1>

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

References

CVE	CVE-2021-28861
XREF	USN:5629-1

Plugin Information

Published: 2022/09/22, 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.

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm5
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm5
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm5
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm5
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm5

168534 - Ubuntu 16.04 ESM : Python vulnerability (USN-5767-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5767-2 advisory.

USN-5767-1 fixed a vulnerability in Python. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5767-2>

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-2022-45061
XREF	USN:5767-2
XREF	IAVA:2023-A-0061-S

Plugin Information

Published: 2022/12/08, Modified: 2024/10/29

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm3
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm3
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm3
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm6
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm6
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm6
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm3
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm3
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm6
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm6

181767 - Ubuntu 16.04 ESM : Python vulnerability (USN-6394-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6394-1 advisory.

It was discovered that Python incorrectly handled certain scripts. 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-6394-1>

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-2022-48560](#)
XREF USN:6394-1

Plugin Information

Published: 2023/09/21, 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.

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm10
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm10
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm10
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm10
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm10

161170 - Ubuntu 16.04 ESM : Rsyslog vulnerabilities (USN-5419-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5419-1 advisory.

It was discovered that Rsyslog improperly handled certain invalid input. An attacker could use this issue to cause Rsyslog to crash.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5419-1>

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/I:H/V:A: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

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-2018-16881
CVE	CVE-2019-17041
CVE	CVE-2019-17042
XREF	USN:5419-1

Plugin Information

Published: 2022/05/13, 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.

- Installed package : rsyslog_8.16.0-1ubuntu3
- Fixed package : rsyslog_8.16.0-1ubuntu3.1+esm1

165524 - Ubuntu 16.04 ESM : SQLite vulnerability (USN-5615-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5615-2 advisory.

USN-5615-1 fixed several vulnerabilities in SQLite. This update provides the corresponding fix for CVE-2020-35525 for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5615-2>

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-2020-35525
XREF	USN:5615-2

Plugin Information

Published: 2022/09/28, Modified: 2024/08/29

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 : libsqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5+esm1

166939 - Ubuntu 16.04 ESM : SQLite vulnerability (USN-5712-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5712-1 advisory.

It was discovered that SQLite did not properly handle large string inputs in certain circumstances. An attacker could possibly use this issue to cause a denial of service or 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-5712-1>

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:5712-1
XREF	IAVA:2022-A-0382-S

Plugin Information

Published: 2022/11/03, 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.

- Installed package : libssqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libssqlite3-0_3.11.0-1ubuntu1.5+esm2

157357 - Ubuntu 16.04 ESM : Samba vulnerability (USN-5260-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5260-3 advisory.

USN-5260-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5260-3>

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: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-2021-44142
XREF	USN:5260-3
XREF	IAVA:2022-A-0054-S

Plugin Information

Published: 2022/02/03, Modified: 2024/08/29

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 : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1
- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34+esm1

161449 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5433-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5433-1 advisory.

It was discovered that Vim incorrectly handled parsing of filenames in its search functionality. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service. (CVE-2021-3973)

It was discovered that Vim incorrectly handled memory when opening and searching the contents of certain files. 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. (CVE-2021-3974)

It was discovered that Vim incorrectly handled memory when opening and editing certain files. 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. (CVE-2021-3984, CVE-2021-4019, CVE-2021-4069)

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. (CVE-2021-4192)

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. (CVE-2022-0261, CVE-2022-0318)

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 with user privileges. (CVE-2022-1154)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5433-1>

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

9.3 (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
CVE	CVE-2021-4192
CVE	CVE-2022-0261
CVE	CVE-2022-0318
CVE	CVE-2022-1154
XREF	USN:5433-1

Plugin Information

Published: 2022/05/24, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm4
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm4
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm4
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm4

170913 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5836-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5836-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5836-1>

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-2023-0054
CVE	CVE-2023-0288
CVE	CVE-2023-0433
XREF	USN:5836-1
XREF	IAVB:2023-B-0016-S
XREF	IAVB:2023-B-0018-S

Plugin Information

Published: 2023/01/31, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm15
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm15
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm15
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm15

157139 - Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5193-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5193-2 advisory.

USN-5193-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5193-2>

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-2021-4008
CVE	CVE-2021-4009
CVE	CVE-2021-4011
XREF	USN:5193-2

Plugin Information

Published: 2022/01/26, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm1

178945 - Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5193-3)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5193-3 advisory.

USN-5193-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5193-3>

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-2021-4011
XREF	USN:5193-3

Plugin Information

Published: 2023/07/27, Modified: 2024/10/29

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 : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm5
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm5

171576 - Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5778-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5778-2 advisory.

USN-5778-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5778-2>

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: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
CVE	CVE-2023-0494
XREF	USN:5778-2

Plugin Information

Published: 2023/02/16, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm5
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm4
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm4

159719 - Ubuntu 16.04 ESM : XZ Utils vulnerability (USN-5378-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5378-3 advisory.

USN-5378-2 fixed a vulnerability in XZ Utils. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5378-3>

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

|

References

CVE	CVE-2022-1271
XREF	USN:5378-3
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/13, Modified: 2024/10/29

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 : liblzma5_5.1.1alpha+20120614-2ubuntu2
- Fixed package : liblzma5_5.1.1alpha+20120614-2ubuntu2.16.04.1+esm1

- Installed package : xz-utils_5.1.1alpha+20120614-2ubuntu2
- Fixed package : xz-utils_5.1.1alpha+20120614-2ubuntu2.16.04.1+esm1

177429 - Ubuntu 16.04 ESM : cups-filters vulnerability (USN-6083-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6083-2 advisory.

USN-6083-1 fixed a vulnerability in cups-filters. This update provides the corresponding update for Ubuntu 16.04 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-6083-2>

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

7.9 (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	CVE-2023-24805
XREF	USN:6083-2

Plugin Information

Published: 2023/06/19, Modified: 2024/10/29

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 : cups-browsed_1.8.3-2ubuntu3.4
- Fixed package : cups-browsed_1.8.3-2ubuntu3.5+esm1
- Installed package : cups-filters_1.8.3-2ubuntu3.4
- Fixed package : cups-filters_1.8.3-2ubuntu3.5+esm1
- Installed package : cups-filters-core-drivers_1.8.3-2ubuntu3.4
- Fixed package : cups-filters-core-drivers_1.8.3-2ubuntu3.5+esm1
- Installed package : libcupsfilters1_1.8.3-2ubuntu3.4
- Fixed package : libcupsfilters1_1.8.3-2ubuntu3.5+esm1
- Installed package : libfontembed1_1.8.3-2ubuntu3.4
- Fixed package : libfontembed1_1.8.3-2ubuntu3.5+esm1

161690 - Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5446-2 advisory.

USN-5446-1 fixed a vulnerability in dpkg. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5446-2>

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

8.5 (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
XREF

[CVE-2022-1664](#)
[USN:5446-2](#)

Plugin Information

Published: 2022/05/31, Modified: 2024/08/29

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 : dpkg_1.18.4ubuntu1.5
- Fixed package : dpkg_1.18.4ubuntu1.7+esm1
- Installed package : dpkg-dev_1.18.4ubuntu1.5
- Fixed package : dpkg-dev_1.18.4ubuntu1.7+esm1
- Installed package : libdpkg-perl_1.18.4ubuntu1.5
- Fixed package : libdpkg-perl_1.18.4ubuntu1.7+esm1

160724 - Ubuntu 16.04 ESM : jbig2dec vulnerabilities (USN-5405-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5405-1 advisory.

It was discovered that jbig2dec incorrectly handled memory when parsing invalid files. An attacker could use this issue to cause jbig2dec to crash, leading to a denial of service. (CVE-2017-9216)

It was discovered that jbig2dec incorrectly handled memory when processing untrusted input. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-12268)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5405-1>

Solution

Update the affected jbig2dec, libjbig2dec0 and / or libjbig2dec0-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-2017-9216
CVE	CVE-2020-12268
XREF	USN:5405-1

Plugin Information

Published: 2022/05/09, 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.

- Installed package : libjbig2dec0_0.12+20150918-1ubuntu0.1
- Fixed package : libjbig2dec0_0.12+20150918-1ubuntu0.1+esm2

161452 - Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5437-1 advisory.

Tobias Stoeckmann discovered that libXfixes 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-5437-1>

Solution

Update the affected libxfixes-dev and / or libxfixes3 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-2016-7944](#)
XREF: [USN:5437-1](#)

Plugin Information

Published: 2022/05/24, 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.

- Installed package : libxfixes3_1:5.0.1-2
- Fixed package : libxfixes3_1:5.0.1-2ubuntu0.1~esm1

171734 - Ubuntu 16.04 ESM : libXpm vulnerabilities (USN-5807-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5807-2 advisory.

USN-5807-1 fixed vulnerabilities in libXpm. This update provides the corresponding updates for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5807-2>

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: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:5807-2

Plugin Information

Published: 2023/02/21, Modified: 2024/08/29

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 : libxpm4_1:3.5.11-1ubuntu0.16.04.1
- Fixed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1+esm1

161330 - Ubuntu 16.04 ESM : libXrandr vulnerabilities (USN-5428-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5428-1 advisory.

Tobias Stoeckmann discovered that libXrandr incorrectly handled certain responses. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2016-7947, CVE-2016-7948)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5428-1>

Solution

Update the affected libxrandr-dev and / or libxrandr2 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-2016-7947
CVE	CVE-2016-7948
XREF	USN:5428-1

Plugin Information

Published: 2022/05/18, 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.

- Installed package : libxrandr2_2:1.5.0-1
- Fixed package : libxrandr2_2:1.5.0-1ubuntu0.1~esm1

161450 - Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5436-1 advisory.

Tobias Stoeckmann discovered that libXrender incorrectly handled certain responses. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2016-7949, CVE-2016-7950)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5436-1>

Solution

Update the affected libxrender-dev and / or libxrender1 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-2016-7949
CVE-2016-7950
XREF-USN:5436-1

Plugin Information

Published: 2022/05/24, Modified: 2024/08/29

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 : libxrender1_1:0.9.9-0ubuntu1
- Fixed package : libxrender1_1:0.9.9-0ubuntu1+esm1

161630 - Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5449-1 advisory.

It was discovered that libXv 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-5449-1>

Solution

Update the affected libxv-dev and / or libxv1 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-2016-5407](#)
XREF USN:5449-1

Plugin Information

Published: 2022/05/27, Modified: 2024/08/29

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 : libxv1_2:1.0.10-1
- Fixed package : libxv1_2:1.0.10-1ubuntu0.16.04.1~esm1

161447 - Ubuntu 16.04 ESM : libpng vulnerabilities (USN-5432-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5432-1 advisory.

It was discovered that libpng incorrectly handled memory when parsing certain PNG files. If a user or automated system were tricked into opening a specially crafted PNG file, an attacker could use this issue to cause libpng to crash, resulting in a denial of service, or possible execute arbitrary code.
(CVE-2017-12652)

Zhengxiong Luo discovered that libpng incorrectly handled memory when parsing certain PNG files. If a user or automated system were tricked into opening a specially crafted PNG file, an attacker could use this issue to cause libpng to crash, resulting in a denial of service, or possible execute arbitrary code.
(CVE-2018-14048)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5432-1>

Solution

Update the affected libpng12-0, libpng12-dev and / or libpng3 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-2017-12652
CVE	CVE-2018-14048
XREF	USN:5432-1

Plugin Information

Published: 2022/05/24, Modified: 2024/08/29

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 : libpng12-0_1.2.54-1ubuntu1.1
- Fixed package : libpng12-0_1.2.54-1ubuntu1.1+esm1

165461 - Ubuntu 16.04 ESM : libvpx vulnerability (USN-5637-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5637-1 advisory.

It was discovered that libvpx incorrectly handled certain WebM media files. A remote attacker could use this issue to crash an application using libvpx under certain conditions, 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-5637-1>

Solution

Update the affected libvpx-dev, libvpx3 and / or vpx-tools 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-2020-0034
XREF	USN:5637-1

Plugin Information

Published: 2022/09/26, 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.

- Installed package : libvpx3_1.5.0-2ubuntu1
- Fixed package : libvpx3_1.5.0-2ubuntu1.1+esm1

150492 - Ubuntu 16.04 ESM : libwebp vulnerabilities (USN-4971-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4971-2 advisory.

USN-4971-1 fixed several vulnerabilities in libwebp. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4971-2>

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

8.5 (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
XREF	USN:4971-2

Plugin Information

Published: 2021/06/10, Modified: 2024/10/29

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 : libwebp5_0.4.4-1
- Fixed package : libwebp5_0.4.4-1ubuntu0.1~esm1

- Installed package : libwebpdemux1_0.4.4-1
- Fixed package : libwebpdemux1_0.4.4-1ubuntu0.1~esm1

- Installed package : libwebpmux1_0.4.4-1
- Fixed package : libwebpmux1_0.4.4-1ubuntu0.1~esm1
```

178444 - Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6078-2 advisory.

USN-6078-1 fixed a vulnerability in libwebp. This update provides the corresponding update for Ubuntu 16.04 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-6078-2>

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-2023-1999
XREF	USN:6078-2

Plugin Information

Published: 2023/07/18, Modified: 2024/10/29

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 : libwebp5_0.4.4-1
- Fixed package : libwebp5_0.4.4-1ubuntu0.1~esm2

- Installed package : libwebpdemux1_0.4.4-1
- Fixed package : libwebpdemux1_0.4.4-1ubuntu0.1~esm2
```

- Installed package : libwebpmpm1_0.4.4-1
- Fixed package : libwebpmpm1_0.4.4-1ubuntu0.1~esm2

149905 - Ubuntu 16.04 ESM : libx11 vulnerability (USN-4966-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-4966-2 advisory.

USN-4966-1 fixed a vulnerability in libx11. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4966-2>

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-2021-31535
XREF	USN:4966-2

Plugin Information

Published: 2021/05/25, Modified: 2024/10/29

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 : libx11-6_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-6_2:1.6.3-1ubuntu2.2+esm1
- Installed package : libx11-data_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-data_2:1.6.3-1ubuntu2.2+esm1
- Installed package : libx11-xcb1_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-xcb1_2:1.6.3-1ubuntu2.2+esm1

168464 - Ubuntu 16.04 ESM : libxml2 vulnerabilities (USN-5760-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5760-2 advisory.

USN-5760-1 fixed vulnerabilities in libxml2. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5760-2>

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-2022-40303
CVE	CVE-2022-40304
XREF	USN:5760-2

Plugin Information

Published: 2022/12/07, Modified: 2024/10/29

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 : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm4

159026 - Ubuntu 16.04 ESM : man-db vulnerability (USN-5334-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5334-1 advisory.

It was discovered that man-db incorrectly handled permission changing operations in its daily cron job, and was therefore affected by a race condition. An 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-5334-1>

Solution

Update the affected man-db 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-2015-1336
XREF	USN:5334-1

Plugin Information

Published: 2022/03/17, 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.

- Installed package : `man-db_2.7.5-1`
- Fixed package : `man-db_2.7.5-1ubuntu0.1~esm1`

161634 - Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5448-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5448-1 advisory.

It was discovered that ncurses was not properly checking array bounds when executing the `fmt_entry` function, which could result in an out-of-bounds write. An attacker could possibly use this issue to execute arbitrary code. (CVE-2017-10684)

It was discovered that ncurses was not properly checking user input, which could result in it being treated as a format argument. An attacker could possibly use this issue to expose sensitive information or to execute arbitrary code. (CVE-2017-10685)

It was discovered that ncurses was incorrectly performing memory management operations and was not blocking access attempts to illegal memory locations. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-11112, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734)

It was discovered that ncurses was not properly performing checks on pointer values before attempting to access the related memory locations, which could lead to NULL pointer dereferencing. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-11113)

It was discovered that ncurses was incorrectly handling loops in libtic, which could lead to the execution of an infinite loop. An attacker could possibly use this issue to cause a denial of service.

(CVE-2017-13728)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5448-1>

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-2017-10684
CVE	CVE-2017-10685
CVE	CVE-2017-11112
CVE	CVE-2017-11113
CVE	CVE-2017-13728
CVE	CVE-2017-13729
CVE	CVE-2017-13730
CVE	CVE-2017-13731
CVE	CVE-2017-13732
CVE	CVE-2017-13733
CVE	CVE-2017-13734
XREF	USN:5448-1

Plugin Information

Published: 2022/05/27, 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.

- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm1
- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm1
- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm1
- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm1
- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm1
- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm1

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

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_2.32.2-1ubuntu1.5
- Fixed package : gir1.2-gdkpixbuf-2.0_2.32.2-1ubuntu1.6+esm1
- Installed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.6+esm1
- Installed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.6+esm1

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

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm7
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm7
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm7
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm7

```
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm7

- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm7
```

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	CVE-2024-3651
XREF	USN:6780-1

Plugin Information

Published: 2024/05/21, 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.

```
- Installed package : python3-idna_2.0-3
- Fixed package : python3-idna_2.0-3ubuntu0.1~esm1
```

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

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_2.52.2-1ubuntu0.3
- Fixed package : gir1.2-soup-2.4_2.52.2-1ubuntu0.3+esm1
- Installed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3+esm1
- Installed package : libsoup2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup2.4-1_2.52.2-1ubuntu0.3+esm1

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
XREF

CVE-2024-7006
USN:6997-1

Plugin Information

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm17

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

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 : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3+esm4
- Installed package : bluez-cups_5.37-0ubuntu5.1

- Fixed package : bluez-cups_5.37-0ubuntu5.3+esm4
- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3+esm4
- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3+esm4

207462 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-7015-2)

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-7015-2 advisory.

USN-7015-1 fixed several vulnerabilities in Python. This update provides one of the corresponding updates for python2.7 for Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS, and a second for python3.5 for Ubuntu 16.04 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-7015-2>

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-2024-6232
CVE	CVE-2024-7592
XREF	USN:7015-2

Plugin Information

Published: 2024/09/19, 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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm10

```
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm10

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm10

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm14

- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm14

- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm14

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm10

- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm10

- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm14

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm14
```

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

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 : `gdb_7.11.1-0ubuntu1~16.5`
- Fixed package : `gdb_7.11.1-0ubuntu1~16.5+esm1`
- Installed package : `gdbserver_7.11.1-0ubuntu1~16.5`
- Fixed package : `gdbserver_7.11.1-0ubuntu1~16.5+esm1`

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_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17

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: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_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30

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_2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.75-1ubuntu0.16.04.7

137179 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4383-1)

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-4383-1 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 addressbar, or execute arbitrary code. (CVE-2020-12405, CVE-2020-12406, CVE-2020-12407, CVE-2020-12408, CVE-2020-12409, CVE-2020-12410, CVE-2020-12411)

It was discovered that NSS showed timing differences when performing DSA signatures. An attacker could potentially exploit this to obtain private keys using a timing attack. (CVE-2020-12399)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4383-1>

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-12399
CVE	CVE-2020-12405
CVE	CVE-2020-12406
CVE	CVE-2020-12407
CVE	CVE-2020-12408
CVE	CVE-2020-12409
CVE	CVE-2020-12410
CVE	CVE-2020-12411
XREF	USN:4383-1
XREF	IAVA:2020-A-0238-S
XREF	IAVA:2020-A-0344-S

Plugin Information

Published: 2020/06/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_77.0.1+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_77.0.1+build1-0ubuntu0.16.04.1
```

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-4408-1 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 permission prompts, or execute arbitrary code. (CVE-2020-12415, CVE-2020-12416, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12422, CVE-2020-12424, CVE-2020-12425, CVE-2020-12426)

It was discovered that when performing add-on updates, certificate chains not terminating with built-in roots were silently rejected. This could result in add-ons becoming outdated. (CVE-2020-12421)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4408-1>

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-12415
CVE	CVE-2020-12416
CVE	CVE-2020-12417
CVE	CVE-2020-12418
CVE	CVE-2020-12419
CVE	CVE-2020-12420
CVE	CVE-2020-12421
CVE	CVE-2020-12422
CVE	CVE-2020-12424
CVE	CVE-2020-12425
CVE	CVE-2020-12426
XREF	USN:4408-1
XREF	IAVA:2020-A-0287-S

Plugin Information

Published: 2020/07/06, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_78.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_78.0.1+build1-0ubuntu0.16.04.1

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: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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_79.0+build1-0ubuntu0.16.04.2
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_79.0+build1-0ubuntu0.16.04.2

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

I

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_84.0+build3-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_84.0+build3-0ubuntu0.16.04.1

138498 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerability (USN-4423-1)**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-4423-1 advisory.

It was discovered that X-Frame-Options could be bypassed in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct clickjacking 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-4423-1>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4423-1

Plugin Information

Published: 2020/07/15, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_78.0.2+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_78.0.2+build2-0ubuntu0.16.04.1

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_82.0.3+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_82.0.3+build1-0ubuntu0.16.04.1

144300 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ImageMagick vulnerabilities (USN-4670-1)

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-4670-1 advisory.

It was discovered that ImageMagick incorrectly handled certain specially crafted image files. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.10. (CVE-2019-19948, CVE-2019-19949)

It was discovered that ImageMagick incorrectly handled certain specially crafted image files. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. (CVE-2020-27560)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4670-1>

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-2019-19948
CVE	CVE-2019-19949
CVE	CVE-2020-27560
XREF	USN:4670-1

Plugin Information

Published: 2020/12/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16

138132 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer vulnerabilities (USN-4407-1)

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-4407-1 advisory.

It was discovered that LibVNCServer incorrectly handled decompressing data. An attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service. (CVE-2019-15680)

It was discovered that an information disclosure vulnerability existed in LibVNCServer when sending a ServerCutText message. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 19.10, Ubuntu 18.04 LTS, and Ubuntu 16.04 LTS. (CVE-2019-15681)

It was discovered that LibVNCServer incorrectly handled cursor shape updates. If a user were tricked into connecting to a malicious server, an attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 19.10, Ubuntu 18.04 LTS, and Ubuntu 16.04 LTS. (CVE-2019-15690, CVE-2019-20788)

It was discovered that LibVNCServer incorrectly handled decoding WebSocket frames. An attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 19.10, Ubuntu 18.04 LTS, and Ubuntu 16.04 LTS. (CVE-2017-18922)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4407-1>

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-2017-18922
CVE	CVE-2019-15680
CVE	CVE-2019-15681
CVE	CVE-2019-15690
CVE	CVE-2019-20788
XREF	USN:4407-1
XREF	IAVA:2020-A-0381

Plugin Information

Published: 2020/07/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.3
- Fixed package : libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.4

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-2020-1436
XREF USN:4489-1

Plugin Information

Published: 2020/09/09, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-117-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:I/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	CVE-2020-14765
CVE	CVE-2020-14769
CVE	CVE-2020-14771
CVE	CVE-2020-14773
CVE	CVE-2020-14775
CVE	CVE-2020-14776
CVE	CVE-2020-14777
CVE	CVE-2020-14785
CVE	CVE-2020-14786
CVE	CVE-2020-14789
CVE	CVE-2020-14790
CVE	CVE-2020-14791
CVE	CVE-2020-14793
CVE	CVE-2020-14794
CVE	CVE-2020-14800
CVE	CVE-2020-14804
CVE	CVE-2020-14809
CVE	CVE-2020-14812
CVE	CVE-2020-14814
CVE	CVE-2020-14821
CVE	CVE-2020-14827
CVE	CVE-2020-14828
CVE	CVE-2020-14829
CVE	CVE-2020-14830
CVE	CVE-2020-14836
CVE	CVE-2020-14837
CVE	CVE-2020-14838
CVE	CVE-2020-14839
CVE	CVE-2020-14844
CVE	CVE-2020-14845
CVE	CVE-2020-14846
CVE	CVE-2020-14848
CVE	CVE-2020-14852
CVE	CVE-2020-14853
CVE	CVE-2020-14860
CVE	CVE-2020-14861
CVE	CVE-2020-14866
CVE	CVE-2020-14867
CVE	CVE-2020-14868
CVE	CVE-2020-14869
CVE	CVE-2020-14870
CVE	CVE-2020-14873
CVE	CVE-2020-14878
CVE	CVE-2020-14888
CVE	CVE-2020-14891
CVE	CVE-2020-14893
XREF	USN:4604-1

Plugin Information

Published: 2020/10/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.32-0ubuntu0.16.04.1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.32-0ubuntu0.16.04.1

146044 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4716-1)

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-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 8.0.23 in Ubuntu 20.04 LTS and Ubuntu 20.10. Ubuntu 16.04 LTS and Ubuntu 18.04 LTS have been updated to MySQL 5.7.33.

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-5-7-33.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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.33-0ubuntu0.16.04.1

- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.33-0ubuntu0.16.04.1

139784 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Net-SNMP vulnerabilities (USN-4471-1)

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/NV:C: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 (CVSS#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_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp-base_5.7.3+dfsg-1ubuntu4.5

- Installed package : libsnmp30_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp30_5.7.3+dfsg-1ubuntu4.5

141913 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Perl vulnerabilities (USN-4602-1)**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-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 : libperl5.22_5.22.1-9ubuntu0.6
- Fixed package : libperl5.22_5.22.1-9ubuntu0.9
- Installed package : perl_5.22.1-9ubuntu0.6
- Fixed package : perl_5.22.1-9ubuntu0.9
- Installed package : perl-base_5.22.1-9ubuntu0.6
- Fixed package : perl-base_5.22.1-9ubuntu0.9
- Installed package : perl-modules-5.22_5.22.1-9ubuntu0.6
- Fixed package : perl-modules-5.22_5.22.1-9ubuntu0.9

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_3.1.2-0ubuntu1.1
- Fixed package : python3-pil_3.1.2-0ubuntu1.6
```

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.14
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.14
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.14
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.14
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.14
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13

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 : lib smbclient _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : lib smbclient _2:4.3.11+dfsg -0ubuntu0.16.04.31
- Installed package : lib wbclient0 _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : lib wbclient0 _2:4.3.11+dfsg -0ubuntu0.16.04.31
- Installed package : python-samba _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : python-samba _2:4.3.11+dfsg -0ubuntu0.16.04.31
- Installed package : samba _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : samba _2:4.3.11+dfsg -0ubuntu0.16.04.31
- Installed package : samba-common _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : samba-common _2:4.3.11+dfsg -0ubuntu0.16.04.31
- Installed package : samba-common-bin _2:4.3.11+dfsg -0ubuntu0.16.04.28
- Fixed package : samba-common-bin _2:4.3.11+dfsg -0ubuntu0.16.04.31

- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.31
- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.31
- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.31

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_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.10

138326 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-4421-1)

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-4421-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked in to 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-2020-12405, CVE-2020-12406, CVE-2020-12410, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420)

It was discovered that Thunderbird would continue an unencrypted connection when configured to use STARTTLS for IMAP if the server responded with PREAUTH. A remote attacker could potentially exploit this to perform a person-in-the-middle attack in order to obtain sensitive information. (CVE-2020-12398)

It was discovered that NSS showed timing differences when performing DSA signatures. An attacker could potentially exploit this to obtain private keys using a timing attack. (CVE-2020-12399)

It was discovered that when performing add-on updates, certificate chains not terminating with built-in roots were silently rejected. This could result in add-ons becoming outdated. (CVE-2020-12421)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4421-1>

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-2020-12398
CVE	CVE-2020-12399
CVE	CVE-2020-12405
CVE	CVE-2020-12406
CVE	CVE-2020-12410
CVE	CVE-2020-12417
CVE	CVE-2020-12418
CVE	CVE-2020-12419
CVE	CVE-2020-12420
CVE	CVE-2020-12421
XREF	USN:4421-1

Plugin Information

Published: 2020/07/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:68.10.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:68.10.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:68.10.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:68.10.0+build1-0ubuntu0.16.04.1

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_3.8.1-0ubuntu9.2
- Fixed package : vino_3.8.1-0ubuntu9.3

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:I/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

Plugin Output

tcp/0

- Installed package : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6

137043 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ca-certificates update (USN-4377-1)

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-4377-1 advisory.

The ca-certificates package contained an expired CA certificate that caused connectivity issues. This update removes the AddTrust External Root CA.

In addition, on Ubuntu 16.04 LTS and Ubuntu 18.04 LTS, this update refreshes the included certificates to those contained in the 20190110 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-4377-1>

Solution

Update the affected ca-certificates and / or ca-certificates-udeb packages.

Risk Factor

High

References

XREF USN:4377-1

Plugin Information**Plugin Output**

tcp/0

- Installed package : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_20190110~16.04.1

136692 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : json-c regression (USN-4360-2)

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-4360-2 advisory.

USN-4360-1 fixed a vulnerability in json-c. The security fix introduced a memory leak in some scenarios. 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-4360-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4360-2

Plugin Information

Published: 2020/05/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libjson-c2_0.11-4ubuntu2
- Fixed package : libjson-c2_0.11-4ubuntu2.5

136607 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif vulnerabilities (USN-4358-1)

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-4358-1 advisory.

It was discovered that libexif incorrectly handled certain tags. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-20030)

It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. (CVE-2020-12767)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4358-1>

Solution

Update the affected libexif-dev and / or libexif12 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-2018-20030
CVE	CVE-2020-12767
XREF	USN:4358-1

Plugin Information

Published: 2020/05/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexif12_0.6.21-2
- Fixed package : libexif12_0.6.21-2ubuntu0.2

142732 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif 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 libexif 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 libexif-dev and / or libexif12 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_0.6.21-2
- Fixed package : libexif12_0.6.21-2ubuntu0.6

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: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_1.0.25+git20150528-1ubuntu2.16.04.1
- Fixed package : libsane_1.0.25+git20150528-1ubuntu2.16.04.3
- Installed package : libsane-common_1.0.25+git20150528-1ubuntu2.16.04.1
- Fixed package : libsane-common_1.0.25+git20150528-1ubuntu2.16.04.3
- Installed package : sane-utils_1.0.25+git20150528-1ubuntu2.16.04.1
- Fixed package : sane-utils_1.0.25+git20150528-1ubuntu2.16.04.3

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

Plugin Output

tcp/0

- Installed package : wpa_supplicant_2.4-0ubuntu6.3
- Fixed package : wpa_supplicant_2.4-0ubuntu6.7

147990 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xterm vulnerability (USN-4746-1)

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-4746-1 advisory.

Tavis Ormandy discovered that xterm incorrectly handled certain character sequences. A remote attacker could use this issue to cause xterm 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-4746-1>

Solution

Update the affected xterm 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-2021-27135
XREF	USN:4746-1

Plugin Information

Plugin Output

tcp/0

- Installed package : xterm_322-1ubuntu1
- Fixed package : xterm_322-1ubuntu1.2

193447 - Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6729-2)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6729-2 advisory.

USN-6729-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6729-2>

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/R:L/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:6729-2
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/04/17, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm12
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm12
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm12
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm12

183607 - Ubuntu 16.04 LTS / 18.04 LTS : Berkeley DB vulnerability (USN-4004-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4004-1 advisory.

It was discovered that Berkeley DB incorrectly handled certain inputs. An attacker could possibly use this issue to read 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-4004-1>

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-2019-8457
XREF	USN:4004-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libdb5.3_5.3.28-11ubuntu0.1
- Fixed package : libdb5.3_5.3.28-11ubuntu0.2

193872 - Ubuntu 16.04 LTS / 18.04 LTS : Dnsmasq vulnerabilities (USN-6657-2)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6657-2 advisory.

USN-6657-1 fixed several vulnerabilities in Dnsmasq. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6657-2>

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:6657-2

Plugin Information

Published: 2024/04/25, Modified: 2024/10/29

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 : dnsmasq-base_2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.90-0ubuntu0.16.04.1+esm1

126068 - Ubuntu 16.04 LTS / 18.04 LTS : Evince update (USN-4024-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4024-1 advisory.

As a security improvement, this update adjusts the AppArmor profile for the Evince thumbnailer to reduce access to the system and adjusts the AppArmor profile for Evince and Evince previewer to limit access to the DBus system bus. Additionally adjust the evince abstraction to disallow writes on parent directories of sensitive 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-4024-1>

Solution

Update the affected packages.

Risk Factor

High

References

XREF

USN:4024-1

Plugin Information

Published: 2019/06/20, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : evince_3.18.2-1ubuntu4.3
- Fixed package : evince_3.18.2-1ubuntu4.5

- Installed package : evince-common_3.18.2-1ubuntu4.3
- Fixed package : evince-common_3.18.2-1ubuntu4.5

- Installed package : libevdocument3-4_3.18.2-1ubuntu4.3
- Fixed package : libevdocument3-4_3.18.2-1ubuntu4.5

- Installed package : libevview3-3_3.18.2-1ubuntu4.3
- Fixed package : libevview3-3_3.18.2-1ubuntu4.5
```

133524 - Ubuntu 16.04 LTS / 18.04 LTS : Exiv2 vulnerability (USN-4270-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4270-1 advisory.

It was discovered that Exiv2 incorrectly handled certain images. 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-4270-1>

Solution

Update the affected exiv2, libexiv2-14 and / or libexiv2-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (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-2019-20421
XREF USN:4270-1

Plugin Information

Published: 2020/02/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.4

126306 - Ubuntu 16.04 LTS / 18.04 LTS : Expat vulnerability (USN-4040-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4040-1 advisory.

It was discovered that Expat incorrectly handled certain XML 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-4040-1>

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-2018-20843
XREF	USN:4040-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/06/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.4

125766 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regression (USN-3991-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3991-2 advisory.

USN-3991-1 fixed vulnerabilities in Firefox. The update caused a regression which resulted in issues when upgrading between Ubuntu releases. 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-3991-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:3991-2

Plugin Information

Published: 2019/06/07, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_67.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_67.0.1+build1-0ubuntu0.16.04.1

125948 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regression (USN-3991-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3991-3 advisory.

USN-3991-1 fixed vulnerabilities in Firefox, and USN-3991-2 fixed a subsequent regression. The update caused an additional regression that resulted in Firefox failing to load correctly after executing it in safe mode. 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-3991-3>

Solution

Update the affected packages.

Risk Factor

High

References

Plugin Information

Published: 2019/06/17, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_67.0.2+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_67.0.2+build2-0ubuntu0.16.04.1

127093 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regressions (USN-4054-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4054-2 advisory.

USN-4054-1 fixed vulnerabilities in Firefox. The update introduced various minor regressions. This update fixes the problems.

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-4054-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4054-2

Plugin Information

Published: 2019/07/26, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_68.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_68.0.1+build1-0ubuntu0.16.04.1

130585 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regressions (USN-4165-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4165-2 advisory.

USN-4165-1 fixed vulnerabilities in Firefox. The update introduced various minor regressions. This update fixes the problems.

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-4165-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4165-2

Plugin Information

Published: 2019/11/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_70.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_70.0.1+build1-0ubuntu0.16.04.1

123078 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-3918-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3918-1 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 via application crash, denial of service via successive FTP authorization prompts or modal alerts, trick the user with confusing permission request prompts, obtain sensitive information, conduct social engineering attacks, or execute arbitrary code. (CVE-2019-9788, CVE-2019-9789, CVE-2019-9790, CVE-2019-9791, CVE-2019-9792, CVE-2019-9795, CVE-2019-9796, CVE-2019-9797, CVE-2019-9799, CVE-2019-9802, CVE-2019-9805, CVE-2019-9806, CVE-2019-9807, CVE-2019-9808, CVE-2019-9809)

A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. If a user were tricked in to opening a specially crafted website with Spectre mitigations disabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2019-9793)

It was discovered that Upgrade-Insecure-Requests was incorrectly enforced for same-origin navigation. An attacker could potentially exploit this to conduct machine-in-the-middle (MITM) attacks. (CVE-2019-9803)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3918-1>

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-2019-9788
CVE	CVE-2019-9789
CVE	CVE-2019-9790
CVE	CVE-2019-9791
CVE	CVE-2019-9792
CVE	CVE-2019-9793
CVE	CVE-2019-9795
CVE	CVE-2019-9796
CVE	CVE-2019-9797
CVE	CVE-2019-9799
CVE	CVE-2019-9802
CVE	CVE-2019-9803
CVE	CVE-2019-9805
CVE	CVE-2019-9806
CVE	CVE-2019-9807
CVE	CVE-2019-9808
CVE	CVE-2019-9809
XREF	USN:3918-1

Plugin Information

Published: 2019/03/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_66.0+build3-0ubuntu0.16.04.2

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_66.0+build3-0ubuntu0.16.04.2

125339 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-3991-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3991-1 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, spoof the browser UI, trick the user in to launching local executable binaries, obtain sensitive information, conduct cross-site scripting (XSS) attacks, or execute arbitrary code. (CVE-2019-11691, CVE-2019-11692, CVE-2019-11693, CVE-2019-11695, CVE-2019-11696, CVE-2019-11699, CVE-2019-11701, CVE-2019-7317, CVE-2019-9800, CVE-2019-9800, CVE-2019-9814, CVE-2019-9817, CVE-2019-9819, CVE-2019-9820, CVE-2019-9821)

It was discovered that pressing certain key combinations could bypass addon installation prompt delays. If a user opened a specially crafted website, an attacker could potentially exploit this to trick them in to installing a malicious extension. (CVE-2019-11697)

It was discovered that history data could be exposed via drag and drop of hyperlinks to and from bookmarks. If a user were tricked in to dragging a specially crafted hyperlink to the bookmark toolbar or sidebar, and subsequently back in to the web content area, an attacker could potentially exploit this to obtain sensitive information. (CVE-2019-11698)

A type confusion bug was discovered with object groups and UnboxedObjects. If a user were tricked in to opening a specially crafted website after enabling the UnboxedObjects feature, an attacker could potentially exploit this to bypass security checks. (CVE-2019-9816)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3991-1>

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-2019-11691
CVE	CVE-2019-11692
CVE	CVE-2019-11693
CVE	CVE-2019-11695
CVE	CVE-2019-11696
CVE	CVE-2019-11697
CVE	CVE-2019-11698
CVE	CVE-2019-11699
CVE	CVE-2019-11701
CVE	CVE-2019-7317
CVE	CVE-2019-9800
CVE	CVE-2019-9814
CVE	CVE-2019-9816
CVE	CVE-2019-9817
CVE	CVE-2019-9819
CVE	CVE-2019-9820
CVE	CVE-2019-9821
XREF	USN:3991-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/05/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_67.0+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_67.0+build2-0ubuntu0.16.04.1

126698 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4054-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4054-1 advisory.

A sandbox escape was discovered in Firefox. If a user were tricked in to installing a malicious language pack, an attacker could exploit this to gain additional privileges. (CVE-2019-9811)

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 same origin restrictions, conduct cross-site scripting (XSS) attacks, conduct cross-site request forgery (CSRF) attacks, spoof origin attributes, spoof the addressbar contents, bypass safebrowsing protections, or execute arbitrary code. (CVE-2019-11709, CVE-2019-11710, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11714, CVE-2019-11715, CVE-2019-11716, CVE-2019-11717, CVE-2019-11718, CVE-2019-11719, CVE-2019-11720, CVE-2019-11721, CVE-2019-11723, CVE-2019-11724, CVE-2019-11725, CVE-2019-11727, CVE-2019-11728, CVE-2019-11729)

It was discovered that Firefox treats all files in a directory as same origin. If a user were tricked in to downloading a specially crafted HTML file, an attacker could potentially exploit this to obtain sensitive information from local files. (CVE-2019-11730)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4054-1>

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-2019-11709
CVE	CVE-2019-11710
CVE	CVE-2019-11711
CVE	CVE-2019-11712
CVE	CVE-2019-11713
CVE	CVE-2019-11714
CVE	CVE-2019-11715
CVE	CVE-2019-11716
CVE	CVE-2019-11717
CVE	CVE-2019-11718
CVE	CVE-2019-11719
CVE	CVE-2019-11720
CVE	CVE-2019-11721
CVE	CVE-2019-11723
CVE	CVE-2019-11724
CVE	CVE-2019-11725
CVE	CVE-2019-11727
CVE	CVE-2019-11728
CVE	CVE-2019-11729
CVE	CVE-2019-11730
CVE	CVE-2019-9811
XREF	USN:4054-1

Plugin Information

Published: 2019/07/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_68.0+build3-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_68.0+build3-0ubuntu0.16.04.1

128521 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4122-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4122-1 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 obtain sensitive information, bypass Content Security Policy (CSP) protections, bypass same-origin restrictions, conduct cross-site scripting (XSS) attacks, cause a denial of service, or execute arbitrary code. (CVE-2019-5849, CVE-2019-11734, CVE-2019-11735, CVE-2019-11737, CVE-2019-11738, CVE-2019-11740, CVE-2019-11742, CVE-2019-11743, CVE-2019-11744, CVE-2019-11746, CVE-2019-11748, CVE-2019-11749, CVE-2019-11750, CVE-2019-11752)

It was discovered that a compromised content process could log in to a malicious Firefox Sync account. An attacker could potentially exploit this, in combination with another vulnerability, to disable the sandbox. (CVE-2019-9812)

It was discovered that addons.mozilla.org and accounts.firefox.com could be loaded in to the same content process. An attacker could potentially exploit this, in combination with another vulnerability that allowed a cross-site scripting (XSS) attack, to modify browser settings. (CVE-2019-11741)

It was discovered that the Forget about this site feature in the history pane removes HTTP Strict Transport Security (HSTS) settings for sites on the pre-load list. An attacker could potentially exploit this to bypass the protections offered by HSTS. (CVE-2019-11747)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4122-1>

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

9.3 (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-2019-11734
CVE	CVE-2019-11735
CVE	CVE-2019-11737
CVE	CVE-2019-11738
CVE	CVE-2019-11740
CVE	CVE-2019-11741
CVE	CVE-2019-11742
CVE	CVE-2019-11743
CVE	CVE-2019-11744
CVE	CVE-2019-11746
CVE	CVE-2019-11747
CVE	CVE-2019-11748

CVE	CVE-2019-11749
CVE	CVE-2019-11750
CVE	CVE-2019-11752
CVE	CVE-2019-5849
CVE	CVE-2019-9812
XREF	USN:4122-1

Plugin Information

Published: 2019/09/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_69.0+build2-0ubuntu0.16.04.4
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_69.0+build2-0ubuntu0.16.04.4

134442 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4299-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4299-1 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, spoof the URL or other browser chrome, obtain sensitive information, bypass Content Security Policy (CSP) protections, or execute arbitrary code. (CVE-2019-20503, CVE-2020-6805, CVE-2020-6806, CVE-2020-6807, CVE-2020-6808, CVE-2020-6810, CVE-2020-6812, CVE-2020-6813, CVE-2020-6814, CVE-2020-6815)

It was discovered that Web Extensions with the all-url permission could access local files. If a user were tricked in to installing a specially crafted extension, an attacker could potentially exploit this to obtain sensitive information. (CVE-2020-6809)

It was discovered that the Devtools' 'Copy as cURL' feature did not fully escape website-controlled data.

If a user were tricked in to using the 'Copy as cURL' feature to copy and paste a command with specially crafted data in to a terminal, an attacker could potentially exploit this to execute arbitrary commands via command injection. (CVE-2020-6811)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4299-1>

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-2019-20503

CVE	CVE-2020-6805
CVE	CVE-2020-6806
CVE	CVE-2020-6807
CVE	CVE-2020-6808
CVE	CVE-2020-6809
CVE	CVE-2020-6810
CVE	CVE-2020-6811
CVE	CVE-2020-6812
CVE	CVE-2020-6813
CVE	CVE-2020-6814
CVE	CVE-2020-6815
XREF	USN:4299-1

Plugin Information

Published: 2020/03/12, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_74.0+build3-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_74.0+build3-0ubuntu0.16.04.1
```

135284 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4323-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4323-1 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, or execute arbitrary code. (CVE-2020-6821, CVE-2020-6822, CVE-2020-6824, CVE-2020-6825, CVE-2020-6826)

It was discovered that extensions could obtain auth codes from OAuth login flows in some circumstances. If a user were tricked in to installing a specially crafted extension, an attacker could potentially exploit this to obtain access to the user's account. (CVE-2020-6823)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4323-1>

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

II

References

CVE	CVE-2020-6821
CVE	CVE-2020-6822
CVE	CVE-2020-6823
CVE	CVE-2020-6824
CVE	CVE-2020-6825
CVE	CVE-2020-6826
XREF	USN:4323-1
XREF	IAVA:2020-A-0128-S

Plugin Information

Published: 2020/04/08, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_75.0+build3-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_75.0+build3-0ubuntu0.16.04.1

183643 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4020-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4020-1 advisory.

A type confusion bug was discovered in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could exploit this by causing a denial of service, or executing 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-4020-1>

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

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-2019-11707
XREF	CISA-KNOWN-EXPLOITED:2022/06/13

XREF IAVA:2019-A-0207-S
XREF USN:4020-1
XREF CEA-ID:CEA-2019-0458

Plugin Information

Published: 2023/10/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_67.0.3+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_67.0.3+build1-0ubuntu0.16.04.1
```

125813 - Ubuntu 16.04 LTS / 18.04 LTS : GLib vulnerability (USN-4014-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4014-1 advisory.

It was discovered that GLib incorrectly handled certain files. An attacker could possibly use this issue to access 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-4014-1>

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-2019-12450
XREF USN:4014-1

Plugin Information

Published: 2019/06/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.2
```

- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.2
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.2

138166 - Ubuntu 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-4416-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4416-1 advisory.

Florian Weimer discovered that the GNU C Library incorrectly handled certain memory operations. 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 16.04 LTS. (CVE-2017-12133)

It was discovered that the GNU C Library incorrectly handled certain SSE2-optimized memmove operations. 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 16.04 LTS. (CVE-2017-18269)

It was discovered that the GNU C Library incorrectly handled certain pathname operations. 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. (CVE-2018-11236)

It was discovered that the GNU C Library incorrectly handled certain AVX-512-optimized mempcpy operations.

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. (CVE-2018-11237)

It was discovered that the GNU C Library incorrectly handled certain hostname lookups. 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. (CVE-2018-19591)

Jakub Wilk discovered that the GNU C Library incorrectly handled certain memalign functions. 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 16.04 LTS. (CVE-2018-6485)

It was discovered that the GNU C Library incorrectly ignored the LD_PREFER_MAP_32BIT_EXEC environment variable after security transitions. A local attacker could use this issue to bypass ASLR restrictions.
(CVE-2019-19126)

It was discovered that the GNU C Library incorrectly handled certain regular expressions. A remote 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 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-9169)

It was discovered that the GNU C Library incorrectly handled certain bit patterns. 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 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2020-10029)

It was discovered that the GNU C Library incorrectly handled certain signal trampolines on PowerPC. 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. (CVE-2020-1751)

It was discovered that the GNU C Library incorrectly handled tilde expansion. 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. (CVE-2020-1752)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4416-1>

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-2017-12133
CVE CVE-2017-18269
CVE CVE-2018-11236
CVE CVE-2018-11237
CVE CVE-2018-19591
CVE CVE-2018-6485
CVE CVE-2019-19126
CVE CVE-2019-9169
CVE CVE-2020-10029
CVE CVE-2020-1751
CVE CVE-2020-1752
XREF USN:4416-1

Plugin Information

Published: 2020/07/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.2
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.2
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.2
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.2
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.2
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.2

128322 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-4111-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4111-1 advisory.

Hiroki Matsukuma discovered that the PDF interpreter in Ghostscript did not properly restrict privileged calls when -dSAFER restrictions were in effect. 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. (CVE-2019-14811, CVE-2019-14812, CVE-2019-14813, CVE-2019-14817)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4111-1>

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

9.4 (CVSS:3.0/E:H/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

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

STIG Severity

I

References

CVE	CVE-2019-14811
CVE	CVE-2019-14812
CVE	CVE-2019-14813
CVE	CVE-2019-14817
XREF	USN:4111-1
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/08/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.11
- Installed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.11
- Installed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.11
- Installed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.11

212086 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-7138-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7138-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-7138-1>

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-2024-46953
CVE	CVE-2024-46955
CVE	CVE-2024-46956
XREF	USN:7138-1
XREF	IAVB:2024-B-0170-S

Plugin Information

Published: 2024/12/05, Modified: 2025/03/28

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.

- Installed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm8
- Installed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm8
- Installed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm8
- Installed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm8

132768 - Ubuntu 16.04 LTS / 18.04 LTS : GnuTLS update (USN-4233-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4233-1 advisory.

As a security improvement, this update marks SHA1 as being untrusted for digital signature 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-4233-1>

Solution

Update the affected packages.

Risk Factor

High

References

XREF	USN:4233-1
------	------------

Plugin Information

Published: 2020/01/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libgnutls-openssl127_3.4.10-4ubuntu1.4
- Fixed package : libgnutls-openssl127_3.4.10-4ubuntu1.6
- Installed package : libgnutls30_3.4.10-4ubuntu1.4
- Fixed package : libgnutls30_3.4.10-4ubuntu1.6

133224 - Ubuntu 16.04 LTS / 18.04 LTS : GnuTLS update (USN-4233-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4233-2 advisory.

USN-4233-1 disabled SHA1 being used for digital signature operations in GnuTLS. In certain network environments, certificates using SHA1 may still be in use. This update adds the %VERIFY_ALLOW_BROKEN and %VERIFY_ALLOW_SIGN_WITH_SHA1 priority strings that can be used to temporarily re-enable SHA1 until certificates can be replaced with a stronger 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-4233-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4233-2

Plugin Information

Published: 2020/01/24, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libgnutls-openssl127_3.4.10-4ubuntu1.4
- Fixed package : libgnutls-openssl127_3.4.10-4ubuntu1.7
- Installed package : libgnutls30_3.4.10-4ubuntu1.4
- Fixed package : libgnutls30_3.4.10-4ubuntu1.7

129289 - Ubuntu 16.04 LTS / 18.04 LTS : IBus regression (USN-4134-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4134-2 advisory.

USN-4134-1 fixed a vulnerability in IBus. The security fix introduced a regression when being used with Qt applications. This update reverts the security fix pending further investigation.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4134-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4134-2

Plugin Information

Published: 2019/09/24, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.1
- Fixed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.3
- Installed package : ibus_1.5.11-1ubuntu2.1
- Fixed package : ibus_1.5.11-1ubuntu2.3
- Installed package : ibus-gtk_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk_1.5.11-1ubuntu2.3
- Installed package : ibus-gtk3_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk3_1.5.11-1ubuntu2.3
- Installed package : libibus-1.0-5_1.5.11-1ubuntu2.1
- Fixed package : libibus-1.0-5_1.5.11-1ubuntu2.3

126815 - Ubuntu 16.04 LTS / 18.04 LTS : LibreOffice vulnerabilities (USN-4063-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4063-1 advisory.

Nils Emmerich discovered that LibreOffice incorrectly handled LibreLogo scripts. If a user were tricked into opening a specially crafted document, a remote attacker could cause LibreOffice to execute arbitrary code. (CVE-2019-9848)

Matei Mal Badanou discovered that LibreOffice incorrectly handled stealth mode. Contrary to expectations, bullet graphics could be retrieved from remote locations when running in stealth mode.

(CVE-2019-9849)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4063-1>

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

9.4 (CVSS:3.0/E:H/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

6.5 (CVSS:2.0/E:H/RL:O/RC:C)

References

CVE-2019-9848
CVE-2019-9849
XREF-USN:4063-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2019/07/19, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial6
- Fixed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial8

- Installed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial8
```

- Installed package : ure_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : ure_5.1.6~rc2-0ubuntu1~xenial8

128027 - Ubuntu 16.04 LTS / 18.04 LTS : LibreOffice vulnerabilities (USN-4102-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4102-1 advisory.

It was discovered that LibreOffice incorrectly handled LibreLogo scripts. If a user were tricked into opening a specially crafted document, a remote attacker could cause LibreOffice to execute arbitrary code.

(CVE-2019-9850, CVE-2019-9851)

It was discovered that LibreOffice incorrectly handled embedded scripts in document files. If a user were tricked into opening a specially crafted document, a remote attacker could possibly execute arbitrary code. (CVE-2019-9852)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4102-1>

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-2019-9850
CVE	CVE-2019-9851
CVE	CVE-2019-9852
XREF	USN:4102-1

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/08/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial6
- Fixed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial9
- Installed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial9
- Installed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial9

```

- Installed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial9

- Installed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial9

- Installed package : ure_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : ure_5.1.6~rc2-0ubuntu1~xenial9

```

125998 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4017-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4017-1 advisory.

Jonathan Looney discovered that the TCP retransmission queue implementation in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. (CVE-2019-11478)

Jonathan Looney discovered that an integer overflow existed in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service (system crash). (CVE-2019-11477)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4017-1>

Solution

Update the affected kernel package.

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-2019-11477
CVE	CVE-2019-11478
XREF	USN:4017-1
XREF	CEA-ID:CEA-2019-0456

Plugin Information

Published: 2019/06/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-52-generic for this advisory.
```

127889 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4094-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4094-1 advisory.

It was discovered that the alarmtimer implementation in the Linux kernel contained an integer overflow vulnerability. A local attacker could use this to cause a denial of service. (CVE-2018-13053)

Wen Xu discovered that the XFS filesystem implementation in the Linux kernel did not properly track inode validations. An attacker could use this to construct a malicious XFS image that, when mounted, could cause a denial of service (system crash). (CVE-2018-13093)

Wen Xu discovered that the f2fs file system implementation in the Linux kernel did not properly validate metadata. An attacker could use this to construct a malicious f2fs image that, when mounted, could cause a denial of service (system crash). (CVE-2018-13097, CVE-2018-13099, CVE-2018-13100, CVE-2018-14614, CVE-2018-14616, CVE-2018-13096, CVE-2018-13098, CVE-2018-14615)

Wen Xu and Po-Ning Tseng discovered that btrfs file system implementation in the Linux kernel did not properly validate metadata. An attacker could use this to construct a malicious btrfs image that, when mounted, could cause a denial of service (system crash). (CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613, CVE-2018-14609)

Wen Xu discovered that the HFS+ filesystem implementation in the Linux kernel did not properly handle malformed catalog data in some situations. An attacker could use this to construct a malicious HFS+ image that, when mounted, could cause a denial of service (system crash). (CVE-2018-14617)

Vasily Averin and Pavel Tikhomirov discovered that the cleancache subsystem of the Linux kernel did not properly initialize new files in some situations. A local attacker could use this to expose sensitive information. (CVE-2018-16862)

Hui Peng and Mathias Payer discovered that the USB subsystem in the Linux kernel did not properly handle size checks when handling an extra USB descriptor. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2018-20169)

It was discovered that a use-after-free error existed in the block layer subsystem of the Linux kernel when certain failure conditions occurred. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-20856)

Eli Biham and Lior Neumann discovered that the Bluetooth implementation in the Linux kernel did not properly validate elliptic curve parameters during Diffie-Hellman key exchange in some situations. An attacker could use this to expose sensitive information. (CVE-2018-5383)

It was discovered that a heap buffer overflow existed in the Marvell Wireless LAN device driver for the Linux kernel. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-10126)

Andrei Vlad Lutas and Dan Lutas discovered that some x86 processors incorrectly handle SWAPGS instructions during speculative execution. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2019-1125)

It was discovered that the PowerPC dlpars implementation in the Linux kernel did not properly check for allocation errors in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-12614)

It was discovered that a NULL pointer dereference vulnerability existed in the Near-field communication (NFC) implementation in the Linux kernel. An attacker could use this to cause a denial of service (system crash). (CVE-2019-12818)

It was discovered that the MDIO bus devices subsystem in the Linux kernel improperly dropped a device reference in an error condition, leading to a use-after-free. An attacker could use this to cause a denial of service (system crash). (CVE-2019-12819)

It was discovered that a NULL pointer dereference vulnerability existed in the Near-field communication (NFC) implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2019-12984)

Jann Horn discovered a use-after-free vulnerability in the Linux kernel when accessing LDT entries in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-13233)

Jann Horn discovered that the ptrace implementation in the Linux kernel did not properly record credentials in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly gain administrative privileges. (CVE-2019-13272)

It was discovered that the Empia EM28xx DVB USB device driver implementation in the Linux kernel contained a use-after-free vulnerability when disconnecting the device. An attacker could use this to cause a denial of service (system crash). (CVE-2019-2024)

It was discovered that the USB video device class implementation in the Linux kernel did not properly validate control bits, resulting in an out of bounds buffer read. A local attacker could use this to possibly expose sensitive information (kernel memory). (CVE-2019-2101)

It was discovered that the Marvell Wireless LAN device driver in the Linux kernel did not properly validate the BSS descriptor. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-3846)

It was discovered that the Appletalk IP encapsulation driver in the Linux kernel did not properly prevent kernel addresses from being copied to user space. A local attacker with the CAP_NET_ADMIN capability could use this to expose sensitive information. (CVE-2018-20511)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4094-1>

Solution

Update the affected kernel 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

9.4 (CVSS:3.0/E:H/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

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

References

CVE	CVE-2018-13053
CVE	CVE-2018-13093
CVE	CVE-2018-13096
CVE	CVE-2018-13097
CVE	CVE-2018-13098
CVE	CVE-2018-13099
CVE	CVE-2018-13100
CVE	CVE-2018-14609
CVE	CVE-2018-14610
CVE	CVE-2018-14611
CVE	CVE-2018-14612
CVE	CVE-2018-14613
CVE	CVE-2018-14614
CVE	CVE-2018-14615
CVE	CVE-2018-14616
CVE	CVE-2018-14617
CVE	CVE-2018-16862
CVE	CVE-2018-20169

CVE	CVE-2018-20511
CVE	CVE-2018-20856
CVE	CVE-2018-5383
CVE	CVE-2019-10126
CVE	CVE-2019-1125
CVE	CVE-2019-12614
CVE	CVE-2019-12818
CVE	CVE-2019-12819
CVE	CVE-2019-12984
CVE	CVE-2019-13233
CVE	CVE-2019-13272
CVE	CVE-2019-2024
CVE	CVE-2019-2101
CVE	CVE-2019-3846
XREF	USN:4094-1
XREF	CISA-KNOWN-EXPLOITED:2022/06/10

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/08/14, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-58-generic for this advisory.

129049 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4135-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4135-1 advisory.

Peter Pi discovered a buffer overflow in the virtio network backend (vhost_net) implementation in the Linux kernel. An attacker in a guest may be able to use this to cause a denial of service (host OS crash) or possibly execute arbitrary code in the host OS. (CVE-2019-14835)

It was discovered that the Linux kernel on PowerPC architectures did not properly handle Facility Unavailable exceptions in some situations. A local attacker could use this to expose sensitive information. (CVE-2019-15030)

It was discovered that the Linux kernel on PowerPC architectures did not properly handle exceptions on interrupts in some situations. A local attacker could use this to expose sensitive information.
(CVE-2019-15031)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4135-1>

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-2019-14835
CVE	CVE-2019-15030
CVE	CVE-2019-15031
XREF	USN:4135-1

Plugin Information

Published: 2019/09/19, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-64-generic for this advisory.
```

130965 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4185-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4185-1 advisory.

Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Giorgi Maisuradze, Moritz Lipp, Michael Schwarz, Daniel Gruss, and Jo Van Bulck discovered that Intel processors using Transactional Synchronization Extensions (TSX) could expose memory contents previously stored in microarchitectural buffers to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11135)

It was discovered that the Intel i915 graphics chipsets allowed userspace to modify page table entries via writes to MMIO from the Blitter Command Streamer and expose kernel memory information. A local attacker could use this to expose sensitive information or possibly elevate privileges. (CVE-2019-0155)

Deepak Gupta discovered that on certain Intel processors, the Linux kernel did not properly perform invalidation on page table updates by virtual guest operating systems. A local attacker in a guest VM could use this to cause a denial of service (host system crash). (CVE-2018-12207)

It was discovered that the Intel i915 graphics chipsets could cause a system hang when userspace performed a read from GT memory mapped input output (MMIO) when the product is in certain low power states. A local attacker could use this to cause a denial of service. (CVE-2019-0154)

Hui Peng discovered that the Atheros AR6004 USB Wi-Fi device driver for the Linux kernel did not properly validate endpoint descriptors returned by the device. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15098)

Ori Nimron discovered that the AX25 network protocol implementation in the Linux kernel did not properly perform permissions checks. A local attacker could use this to create a raw socket. (CVE-2019-17052)

Ori Nimron discovered that the IEEE 802.15.4 Low-Rate Wireless network protocol implementation in the Linux kernel did not properly perform permissions checks. A local attacker could use this to create a raw socket. (CVE-2019-17053)

Ori Nimron discovered that the Appletalk network protocol implementation in the Linux kernel did not properly perform permissions checks. A local attacker could use this to create a raw socket.
(CVE-2019-17054)

Ori Nimron discovered that the modular ISDN network protocol implementation in the Linux kernel did not properly perform permissions checks. A local attacker could use this to create a raw socket.
(CVE-2019-17055)

Ori Nimron discovered that the Near field Communication (NFC) network protocol implementation in the Linux kernel did not properly perform permissions checks. A local attacker could use this to create a raw socket. (CVE-2019-17056)

Nico Waisman discovered that a buffer overflow existed in the Realtek Wi-Fi driver for the Linux kernel when handling Notice of Absence frames. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-17666)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4185-1>

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-2018-12207
CVE	CVE-2019-0154
CVE	CVE-2019-0155
CVE	CVE-2019-11135
CVE	CVE-2019-15098
CVE	CVE-2019-17052
CVE	CVE-2019-17053
CVE	CVE-2019-17054
CVE	CVE-2019-17055
CVE	CVE-2019-17056
CVE	CVE-2019-17666
XREF	USN:4185-1

Plugin Information

Published: 2019/11/13, Modified: 2024/08/28

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-69-generic for this advisory.

131564 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4210-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4210-1 advisory.

It was discovered that a buffer overflow existed in the 802.11 Wi-Fi configuration interface for the Linux kernel when handling beacon settings. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-16746)

Nicolas Waisman discovered that the WiFi driver stack in the Linux kernel did not properly validate SSID lengths. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-17133)

It was discovered that the ADIS16400 IIO IMU Driver for the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19060)

It was discovered that the Intel OPA Gen1 Infiniband Driver for the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19065)

It was discovered that the Cascoda CA8210 SPI 802.15.4 wireless controller driver for the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19075)

Nicolas Waisman discovered that the Chelsio T4/T5 RDMA Driver for the Linux kernel performed DMA from a kernel stack. A local attacker could use this to cause a

denial of service (system crash).
(CVE-2019-17075)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4210-1>

Solution

Update the affected kernel 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-2019-16746
CVE	CVE-2019-17075
CVE	CVE-2019-17133
CVE	CVE-2019-19060
CVE	CVE-2019-19065
CVE	CVE-2019-19075
XREF	USN:4210-1

Plugin Information

Published: 2019/12/03, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-72-generic for this advisory.

137300 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4390-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4390-1 advisory.

It was discovered that the F2FS file system implementation in the Linux kernel did not properly perform bounds checking on xattrs in some situations. A local attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2020-0067)

It was discovered that memory contents previously stored in microarchitectural special registers after RDRAND, RDSEED, and SGX EGETKEY read operations on Intel client and Xeon E3 processors may be briefly exposed to processes on the same or different processor cores. A local attacker could use this to expose sensitive information. (CVE-2020-0543)

Piotr Krysiuk discovered that race conditions existed in the file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-12114)

It was discovered that the USB subsystem's scatter-gather implementation in the Linux kernel did not properly take data references in some situations, leading to a use-after-free. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2020-12464)

Xiumei Mu discovered that the IPSec implementation in the Linux kernel did not properly encrypt IPv6 traffic in some situations. An attacker could use this to expose sensitive information. (CVE-2020-1749)

Dmitry Vyukov discovered that the SELinux netlink security hook in the Linux kernel did not validate messages in some situations. A privileged attacker could use this to bypass SELinux netlink restrictions. (CVE-2020-10751)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4390-1>

Solution

Update the affected kernel package.

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

7.2 (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-2020-0067
CVE	CVE-2020-0543
CVE	CVE-2020-10751
CVE	CVE-2020-12114
CVE	CVE-2020-12464
CVE	CVE-2020-1749
XREF	USN:4390-1

Plugin Information

Published: 2020/06/10, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-106-generic for this advisory.

138139 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4414-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4414-1 advisory.

It was discovered that the network block device (nbd) implementation in the Linux kernel did not properly check for error conditions in some situations. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-16089)

It was discovered that the btrfs file system implementation in the Linux kernel did not properly validate file system metadata in some situations. An attacker could use this to construct a malicious btrfs image that, when mounted, could cause a denial of service (system crash). (CVE-2019-19036, CVE-2019-19318, CVE-2019-19813, CVE-2019-19816)

It was discovered that the btrfs implementation in the Linux kernel did not properly detect that a block was marked dirty in some situations. An attacker could use this to specially craft a file system image that, when unmounted, could cause a denial of service (system crash). (CVE-2019-19377)

It was discovered that the kernel->user space relay implementation in the Linux kernel did not properly check return values in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-19462)

Matthew Sheets discovered that the SELinux network label handling implementation in the Linux kernel could be coerced into de-referencing a NULL pointer. A remote attacker could use this to cause a denial of service (system crash). (CVE-2020-10711)

It was discovered that the SCSI generic (sg) driver in the Linux kernel did not properly handle certain error conditions correctly. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2020-12770)

It was discovered that the USB Gadget device driver in the Linux kernel did not validate arguments passed from configs in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2020-13143)

It was discovered that the efi subsystem in the Linux kernel did not handle memory allocation failures during early boot in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-12380)

It was discovered that the btrfs file system in the Linux kernel in some error conditions could report register information to the dmesg buffer. A local attacker could possibly use this to expose sensitive information. (CVE-2019-19039)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4414-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR: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:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-12380
CVE	CVE-2019-16089
CVE	CVE-2019-19036
CVE	CVE-2019-19039
CVE	CVE-2019-19318
CVE	CVE-2019-19377
CVE	CVE-2019-19462
CVE	CVE-2019-19813
CVE	CVE-2019-19816
CVE	CVE-2020-10711
CVE	CVE-2020-12770
CVE	CVE-2020-13143
XREF	USN:4414-1

Plugin Information

Published: 2020/07/06, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-107-generic for this advisory.

138835 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4426-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4426-1 advisory.

Jason A. Donenfeld discovered that the ACPI implementation in the Linux kernel did not properly restrict loading SSDT code from an EFI variable. A privileged attacker could use this to bypass Secure Boot lockdown restrictions and execute arbitrary code in the kernel. (CVE-2019-20908)

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)

Mauricio Faria de Oliveira discovered that the aufs implementation in the Linux kernel improperly managed inode reference counts in the vfs_sub_dentry_open() method. A local attacker could use this vulnerability to cause a denial of service. (CVE-2020-11935)

Jason A. Donenfeld discovered that the ACPI implementation in the Linux kernel did not properly restrict loading ACPI tables via configs. A privileged attacker could use this to bypass Secure Boot lockdown restrictions and execute arbitrary code in the kernel. (CVE-2020-15780)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4426-1>

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-2019-20908
CVE	CVE-2020-10757
CVE	CVE-2020-11935
CVE	CVE-2020-15780
XREF	USN:4426-1

Plugin Information

Published: 2020/07/22, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-112-generic for this advisory.

140722 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4526-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4526-1 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 ADIS16400 IIO IMU Driver for the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19061)

It was discovered that the AMD Audio Coprocessor driver for the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker with the ability to load modules could use this to cause a denial of service (memory exhaustion). (CVE-2019-19067)

It was discovered that the Atheros HTC based wireless driver in the Linux kernel did not properly deallocate in certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-19073, CVE-2019-19074)

It was discovered that the F2FS file system in the Linux kernel did not properly perform bounds checking in some situations, leading to an out-of- bounds read. A local attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2019-9445)

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 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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4526-1>

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-2019-9445
CVE	CVE-2019-18808
CVE	CVE-2019-19054
CVE	CVE-2019-19061
CVE	CVE-2019-19067
CVE	CVE-2019-19073

CVE	CVE-2019-19074
CVE	CVE-2020-12888
CVE	CVE-2020-14356
CVE	CVE-2020-16166
XREF	USN:4526-1

Plugin Information

Published: 2020/09/22, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-118-generic for this advisory.

143445 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4660-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4660-1 advisory.

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 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)

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)

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-4660-1>

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-2020-4788
CVE	CVE-2020-14351
CVE	CVE-2020-14390
CVE	CVE-2020-25211
CVE	CVE-2020-25284
CVE	CVE-2020-25285
CVE	CVE-2020-25641
CVE	CVE-2020-25643
CVE	CVE-2020-25645
CVE	CVE-2020-28915
XREF	USN:4660-1

Plugin Information

Published: 2020/12/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-126-generic for this advisory.
```

144749 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4680-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4680-1 advisory.

It was discovered that debugfs in the Linux kernel as used by blktrace contained a use-after-free in some situations. A privileged local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-19770)

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 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)

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)

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-4680-1>

Solution

Update the affected kernel package.

Risk Factor

High

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

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-2019-19770
CVE	CVE-2020-0423
CVE	CVE-2020-10135
CVE	CVE-2020-25656
CVE	CVE-2020-25668
CVE	CVE-2020-25705
CVE	CVE-2020-27675
CVE	CVE-2020-27777
CVE	CVE-2020-28974
XREF	USN:4680-1
XREF	CEA-ID:CEA-2020-0138

Plugin Information

Published: 2021/01/06, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-129-generic for this advisory.

147983 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4749-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4749-1 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 the memory management subsystem in the Linux kernel did not properly handle copy-on-write operations in some situations. A local

attacker could possibly use this to gain unintended write access to read-only memory pages. (CVE-2020-29374)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4749-1>

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: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-2020-28941
CVE	CVE-2020-29374
CVE	CVE-2020-29568
CVE	CVE-2020-29569
CVE	CVE-2020-29660
CVE	CVE-2020-29661
XREF	USN:4749-1

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-136-generic for this advisory.

147992 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4877-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4877-1 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)

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-4877-1>

Solution

Update the affected kernel package.

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:I/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-36158
CVE	CVE-2021-3178
XREF	USN:4877-1

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-137-generic for this advisory.

148691 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4916-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4916-1 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)

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-4916-1>

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-2021-3493
CVE	CVE-2021-29154
XREF	USN:4916-1
XREF	CISA-KNOWN-EXPLOITED:2022/11/10

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2021/04/16, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-142-generic for this advisory.

192222 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6701-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6701-1 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)

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 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 ext4 file system implementation in the Linux kernel did not properly handle block device modification while it is mounted. A privileged attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-34256)

Eric Dumazet discovered that the netfilter subsystem in the Linux kernel did not properly handle DCCP conntrack buffers in certain situations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2023-39197)

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)

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 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)

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 ext4 file system implementation in the Linux kernel did not properly handle the remount operation 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 expose sensitive information. (CVE-2024-0775)

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-6701-1>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/NC:H/Vl: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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-2002
CVE	CVE-2023-3006
CVE	CVE-2023-4132
CVE	CVE-2023-6121
CVE	CVE-2023-23000
CVE	CVE-2023-34256
CVE	CVE-2023-39197
CVE	CVE-2023-46838
CVE	CVE-2023-51781
CVE	CVE-2024-0775
CVE	CVE-2024-1086
CVE	CVE-2024-24855
XREF	USN:6701-1
XREF	CISA-KNOWN-EXPLOITED:2024/06/20

Plugin Information

Published: 2024/03/18, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-223-generic for this advisory.

131013 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability and regression (USN-4185-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4185-3 advisory.

USN-4185-1 fixed vulnerabilities in the Linux kernel. It was discovered that the kernel fix for CVE-2019-0155 (i915 missing Blitter Command Streamer check) was incomplete on 64-bit Intel x86 systems.

Also, the update introduced a regression that broke KVM guests where extended page tables (EPT) are disabled or not supported. This update addresses both issues.

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-4185-3>

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-2019-0155
XREF	USN:4185-3

Plugin Information

Published: 2019/11/14, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-70-generic for this advisory.

124152 - Ubuntu 16.04 LTS / 18.04 LTS : NTFS-3G update (USN-3914-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3914-2 advisory.

USN-3914-1 fixed vulnerabilities in NTFS-3G. As an additional hardening measure, this update removes the setuid bit from the ntfs-3g binary.

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

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

See Also

<https://ubuntu.com/security/notices/USN-3914-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:3914-2

Plugin Information

Published: 2019/04/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.3

140176 - Ubuntu 16.04 LTS / 18.04 LTS : Net-SNMP regression (USN-4471-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4471-2 advisory.

USN-4471-1 fixed a vulnerability in Net-SNMP. The updated introduced a regression making nsExtendCacheTime not settable. This update fixes the problem adding the cacheTime feature flag.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4471-2>

Solution

Update the affected packages.

Risk Factor

High

STIG Severity

I

References

XREF USN:4471-2

XREF

IAVA:2020-A-0384-S

Plugin Information

Published: 2020/09/02, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libsnmp-base_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp-base_5.7.3+dfsg-1ubuntu4.6

- Installed package : libsnmp30_5.7.3+dfsg-1ubuntu4.2
- Fixed package : libsnmp30_5.7.3+dfsg-1ubuntu4.6

216430 - Ubuntu 16.04 LTS / 18.04 LTS : OpenSSH vulnerability (USN-7270-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7270-2 advisory.

USN-7270-1 fixed a vulnerability in OpenSSH. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-7270-2>

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
XREF	USN:7270-2
XREF	IAVA:2025-A-0126-S

Plugin Information

Published: 2025/02/18, Modified: 2025/04/17

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 : openssh-client_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-client_1:7.2p2-4ubuntu2.10+esm7
- Installed package : openssh-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-server_1:7.2p2-4ubuntu2.10+esm7
- Installed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm7

127042 - Ubuntu 16.04 LTS / 18.04 LTS : Patch vulnerabilities (USN-4071-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4071-1 advisory.

It was discovered that Patch incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information. (CVE-2019-13636)

It was discovered that Patch incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-13638)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4071-1>

Solution

Update the affected patch package.

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-2019-13636
CVE	CVE-2019-13638
XREF	USN:4071-1

Plugin Information

Published: 2019/07/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : patch_2.7.5-1ubuntu0.16.04.1
- Fixed package : patch_2.7.5-1ubuntu0.16.04.2

133550 - Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4272-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4272-1 advisory.

It was discovered that Pillow incorrectly handled certain images. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-16865, CVE-2019-19911)

It was discovered that Pillow incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code. (CVE-2020-5312)

It was discovered that Pillow incorrectly handled certain TIFF images. An attacker could possibly use this issue to cause a crash. This issue only affected Ubuntu 19.10. (CVE-2020-5310)

It was discovered that Pillow incorrectly handled certain SGI images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. This issue only affected Ubuntu 18.04 and Ubuntu 19.10.
(CVE-2020-5311)

It was discovered that Pillow incorrectly handled certain PCX images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2020-5312)

It was discovered that Pillow incorrectly handled certain Flip images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2020-5313)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4272-1>

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-2019-16865
CVE	CVE-2019-19911
CVE	CVE-2020-5310
CVE	CVE-2020-5311
CVE	CVE-2020-5312
CVE	CVE-2020-5313
XREF	USN:4272-1

Plugin Information

Published: 2020/02/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_3.1.2-0ubuntu1.1

- Fixed package : python3-pil_3.1.2-0ubuntu1.3

147995 - Ubuntu 16.04 LTS / 18.04 LTS : Python 2.7 vulnerability (USN-4754-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4754-4 advisory.

USN-4754-1 fixed vulnerabilities in Python. Because of a regression, a subsequent update removed the fix for CVE-2021-3177. This update reinstates the security fix for CVE-2021-3177.

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-4754-4>

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-2021-3177
XREF	USN:4754-4

Plugin Information

Published: 2021/03/23, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18

125705 - Ubuntu 16.04 LTS / 18.04 LTS : Qt vulnerabilities (USN-4003-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4003-1 advisory.

It was discovered that Qt incorrectly handled certain XML documents. A remote attacker could use this issue with a specially crafted XML document to cause Qt to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2018-15518)

It was discovered that Qt incorrectly handled certain GIF images. A remote attacker could use this issue with a specially crafted GIF image to cause Qt to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2018-19870)

It was discovered that Qt incorrectly handled certain BMP images. A remote attacker could use this issue with a specially crafted BMP image to cause Qt to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2018-19873)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4003-1>

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-2018-15518
CVE	CVE-2018-19870
CVE	CVE-2018-19873
XREF	USN:4003-1

Plugin Information

Published: 2019/06/04, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libqt5core5a_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5core5a_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5dbus5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5dbus5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5gui5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5gui5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5network5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5network5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5opengl5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5opengl5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5printsupport5_5.5.1+dfsg-16ubuntu7.5

- Fixed package : libqt5printsupport5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5sql5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5sql5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5sql5-sqlite_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5sql5-sqlite_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5test5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5test5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5widgets5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5widgets5_5.5.1+dfsg-16ubuntu7.6
- Installed package : libqt5xml5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5xml5_5.5.1+dfsg-16ubuntu7.6

133551 - Ubuntu 16.04 LTS / 18.04 LTS : ReportLab vulnerability (USN-4273-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4273-1 advisory.

It was discovered that ReportLab incorrectly handled certain XML documents. If a user or automated system were tricked into processing a specially crafted document, 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-4273-1>

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-2019-17626
XREF	USN:4273-1

Plugin Information

Published: 2020/02/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-renderpm_3.3.0-1
- Fixed package : python3-renderpm_3.3.0-1ubuntu0.1
- Installed package : python3-reportlab_3.3.0-1
- Fixed package : python3-reportlab_3.3.0-1ubuntu0.1

- Installed package : python3-reportlab-accel_3.3.0-1
- Fixed package : python3-reportlab-accel_3.3.0-1ubuntu0.1

126065 - Ubuntu 16.04 LTS / 18.04 LTS : SQLite vulnerabilities (USN-4019-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4019-1 advisory.

It was discovered that SQLite incorrectly handled certain SQL files. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. This issue only affected Ubuntu 16.04 LTS.

(CVE-2017-2518, CVE-2017-2520)

It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 18.10.

(CVE-2018-20505)

It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 18.10. (CVE-2018-20346, CVE-2018-20506)

It was discovered that SQLite incorrectly handled certain inputs. An attacker could possibly use this issue to access sensitive information. (CVE-2019-8457)

It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to access sensitive information. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 18.10. (CVE-2019-9936)

It was discovered that SQLite incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 18.10. (CVE-2019-9937)

It was discovered that SQLite incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS. (CVE-2016-6153)

It was discovered that SQLite incorrectly handled certain databases. An attacker could possibly use this issue to access sensitive information. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-10989)

It was discovered that SQLite incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-13685)

It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. This issue only affected Ubuntu 16.04 LTS.

(CVE-2017-2519)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4019-1>

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-2016-6153
CVE	CVE-2017-10989
CVE	CVE-2017-13685
CVE	CVE-2017-2518
CVE	CVE-2017-2519
CVE	CVE-2017-2520
CVE	CVE-2018-20346
CVE	CVE-2018-20505
CVE	CVE-2018-20506
CVE	CVE-2019-8457
CVE	CVE-2019-9936
XREF	CVE-2019-9937
	USN:4019-1

Plugin Information

Published: 2019/06/20, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.2
```

140640 - Ubuntu 16.04 LTS / 18.04 LTS : Samba vulnerability (USN-4510-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4510-1 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.

This update fixes the issue by changing the server schannel setting to default to yes, instead of auto, which will force a secure netlogon channel. This may result in compatibility issues with older devices. A future update may allow a finer-grained control over this setting.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4510-1>

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:4510-1
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: 2020/09/17, Modified: 2024/11/29

Plugin Output

tcp/0

- Installed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.30
- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.30

129882 - Ubuntu 16.04 LTS / 18.04 LTS : Sudo vulnerability (USN-4154-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4154-1 advisory.

Joe Vennix discovered that Sudo incorrectly handled certain user IDs. An attacker could potentially exploit this to execute arbitrary commands as the root 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-4154-1>

Solution

Update the affected sudo and / or sudo-ldap 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-14287
XREF	USN:4154-1
XREF	IAVA:2019-A-0378-S

Exploitable With

Core Impact (true)

Plugin Information

Published: 2019/10/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : sudo_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.8

125545 - Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-3997-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3997-1 advisory.

Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass same-origin protections, or execute arbitrary code. (CVE-2019-18511, CVE-2019-11691, CVE-2019-11692, CVE-2019-11693, CVE-2019-9797, CVE-2019-9800, CVE-2019-9817, CVE-2019-9819, CVE-2019-9820)

Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit these to cause a denial of service, or execute arbitrary code. (CVE-2019-5798, CVE-2019-7317)

A type confusion bug was discovered with object groups and UnboxedObjects. If a user were tricked in to opening a specially crafted website in a browsing context after enabling the UnboxedObjects feature, an attacker could potentially exploit this to bypass security checks. (CVE-2019-9816)

It was discovered that history data could be exposed via drag and drop of hyperlinks to and from bookmarks. If a user were tricked in to dragging a specially crafted hyperlink to a bookmark toolbar or sidebar, and subsequently back in to the web content area, an attacker could potentially exploit this to obtain sensitive information. (CVE-2019-11698)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3997-1>

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 (CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.2 (CVSS:2.0/E:F/RL:OF/RC:C)

References

CVE	CVE-2018-18511
CVE	CVE-2019-11691
CVE	CVE-2019-11692
CVE	CVE-2019-11693
CVE	CVE-2019-11698
CVE	CVE-2019-5798
CVE	CVE-2019-7317
CVE	CVE-2019-9797
CVE	CVE-2019-9800
CVE	CVE-2019-9816
CVE	CVE-2019-9817
CVE	CVE-2019-9819
CVE	CVE-2019-9820
XREF	USN:3997-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/05/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:60.7.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.7.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.7.0+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.7.0+build1-0ubuntu0.16.04.1

126099 - Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4028-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4028-1 advisory.

Multiple memory safety issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted message, 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4028-1>

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-2019-11703
CVE	CVE-2019-11704
CVE	CVE-2019-11705
CVE	CVE-2019-11706
XREF	USN:4028-1

Plugin Information

Published: 2019/06/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:60.7.1+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.7.1+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.7.1+build1-0ubuntu0.16.04.1
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.7.1+build1-0ubuntu0.16.04.1

126816 - Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4064-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4064-1 advisory.

A sandbox escape was discovered in Thunderbird. If a user were tricked in to installing a malicious language pack, an attacker could exploit this to gain additional privileges. (CVE-2019-9811)

Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass same origin restrictions, conduct cross-site scripting (XSS) attacks, spoof origin attributes, or execute arbitrary code. (CVE-2019-11709, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11715, CVE-2019-11717)

It was discovered that NSS incorrectly handled importing certain curve25519 private keys. An attacker could exploit this issue to cause Thunderbird to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2019-11719)

It was discovered that NSS incorrectly handled certain p256-ECDH public keys. An attacker could possibly exploit this issue to cause Thunderbird to crash, resulting in a denial of service. (CVE-2019-11729)

It was discovered that Thunderbird treats all files in a directory as same origin. If a user were tricked in to downloading a specially crafted HTML file, an attacker could potentially exploit this to obtain sensitive information from local files. (CVE-2019-11730)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4064-1>

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-2019-11709
CVE	CVE-2019-11711
CVE	CVE-2019-11712
CVE	CVE-2019-11713
CVE	CVE-2019-11715
CVE	CVE-2019-11717
CVE	CVE-2019-11719
CVE	CVE-2019-11729
CVE	CVE-2019-11730
CVE	CVE-2019-9811
XREF	USN:4064-1

Plugin Information

Published: 2019/07/19, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:60.8.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.8.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.8.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.8.0+build1-0ubuntu0.16.04.2

183629 - Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4150-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4150-1 advisory.

It was discovered that encrypted S/MIME parts in a multipart message can leak plaintext contents when included in a HTML reply or forward in some circumstances. If a user were tricked into replying to or forwarding a specially crafted message, an attacker could potentially exploit this to obtain sensitive information. (CVE-2019-11739)

Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to obtain sensitive information, conduct cross-site scripting (XSS) attack, cause a denial of service, or execute arbitrary code. (CVE-2019-11740, CVE-2019-11742, CVE-2019-11743, CVE-2019-11744, CVE-2019-11746, CVE-2019-11752)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4150-1>

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-2019-11739
CVE	CVE-2019-11740
CVE	CVE-2019-11742
CVE	CVE-2019-11743
CVE	CVE-2019-11744
CVE	CVE-2019-11746
CVE	CVE-2019-11752
XREF	IAVA:2019-A-0324-S
XREF	IAVA:2019-A-0342-S
XREF	USN:4150-1

Plugin Information

Published: 2023/10/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:60.9.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:60.9.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:60.9.0+build1-0ubuntu0.16.04.2
- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:60.9.0+build1-0ubuntu0.16.04.2

201110 - Ubuntu 16.04 LTS / 18.04 LTS : Wget vulnerability (USN-6852-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6852-2 advisory.

USN-6852-1 fixed a vulnerability in Wget. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6852-2>

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:6852-2

Plugin Information

Published: 2024/06/27, Modified: 2024/10/29

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 : wget_1.17.1-1ubuntu1.4
- Fixed package : wget_1.17.1-1ubuntu1.5+esm1
```

130427 - Ubuntu 16.04 LTS / 18.04 LTS : Whoopsie regression (USN-4170-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4170-2 advisory.

USN-4170-1 fixed a vulnerability in Whoopsie. The update caused Whoopsie to crash when sending reports. 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-4170-2>

Solution

Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie packages.

Risk Factor

High

References

XREF USN:4170-2

Plugin Information

Published: 2019/10/31, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libwhoopsie0_0.2.52.5
- Fixed package : libwhoopsie0_0.2.52.5ubuntu0.3

- Installed package : whoopsie_0.2.52.5
- Fixed package : whoopsie_0.2.52.5ubuntu0.3

130513 - Ubuntu 16.04 LTS / 18.04 LTS : Whoopsie regression (USN-4170-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4170-3 advisory.

USN-4170-1 fixed a vulnerability in Whoopsie and USN-4170-2 fixed a subsequent regression. That update was incomplete and could still result in Whoopsie potentially crashing when uploading crash reports on some architectures.

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-4170-3>

Solution

Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie packages.

Risk Factor

High

References

XREF USN:4170-3

Plugin Information

Published: 2019/11/05, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libwhoopsie0_0.2.52.5
- Fixed package : libwhoopsie0_0.2.52.5ubuntu0.4

- Installed package : whoopsie_0.2.52.5
- Fixed package : whoopsie_0.2.52.5ubuntu0.4

126503 - Ubuntu 16.04 LTS / 18.04 LTS : bzip2 regression (USN-4038-3)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4038-3 advisory.

USN-4038-1 fixed a vulnerability in bzip2. The update introduced a regression causing bzip2 to incorrectly raise CRC errors for some files.

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-4038-3>

Solution

Update the affected bzip2, libbz2-1.0 and / or libbz2-dev packages.

Risk Factor

High

References

XREF USN:4038-3

Plugin Information

Published: 2019/07/05, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : bzip2_1.0.6-8
- Fixed package : bzip2_1.0.6-8ubuntu0.2

- Installed package : libbz2-1.0_1.0.6-8
- Fixed package : libbz2-1.0_1.0.6-8ubuntu0.2

126305 - Ubuntu 16.04 LTS / 18.04 LTS : bzip2 vulnerabilities (USN-4038-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4038-1 advisory.

Aladdin Mubaied discovered that bzip2 incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS. (CVE-2016-3189)

It was discovered that bzip2 incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-12900)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4038-1>

Solution

Update the affected bzip2, libbz2-1.0 and / or libbz2-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)

STIG Severity

I

References

CVE	CVE-2016-3189
CVE	CVE-2019-12900
XREF	USN:4038-1
XREF	IAVA:2020-A-0482

Plugin Information

Published: 2019/06/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : bzip2_1.0.6-8
- Fixed package : bzip2_1.0.6-8ubuntu0.1
- Installed package : libbz2-1.0_1.0.6-8
- Fixed package : libbz2-1.0_1.0.6-8ubuntu0.1

128754 - Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerabilities (USN-4129-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4129-1 advisory.

Thomas Vegas discovered that curl incorrectly handled memory when using Kerberos over FTP.

A remote attacker could use this issue to crash curl, resulting in a denial of service. (CVE-2019-5481)

Thomas Vegas discovered that curl incorrectly handled memory during TFTP transfers. A remote attacker could use this issue to crash curl, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2019-5482)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4129-1>

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-2019-5481
CVE	CVE-2019-5482
XREF	USN:4129-1

Plugin Information

Published: 2019/09/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.14
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.14

192630 - Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6718-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6718-2 advisory.

USN-6718-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6718-2>

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-2024-2398
XREF	USN:6718-2
XREF	IAVA:2024-A-0185-S

Plugin Information

Published: 2024/03/27, 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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm12

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm12

125811 - Ubuntu 16.04 LTS / 18.04 LTS : elfutils vulnerabilities (USN-4012-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4012-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4012-1>

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-2018-16062
CVE	CVE-2018-16402
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
XREF	USN:4012-1

Plugin Information

Published: 2019/06/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libelf1_0.165-3ubuntu1.1
- Fixed package : libelf1_0.165-3ubuntu1.2

136604 - Ubuntu 16.04 LTS / 18.04 LTS : file regression (USN-3911-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3911-2 advisory.

USN-3911-1 fixed vulnerabilities in file. One of the backported security fixes introduced a regression that caused the interpreter string to be truncated. 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-3911-2>

Solution

Update the affected packages.

Risk Factor

High

References

XREF	USN:3911-2
------	----------------------------

Plugin Information

Published: 2020/05/14, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : file_1:5.25-2ubuntu1.1
 - Fixed package : file_1:5.25-2ubuntu1.4
-
- Installed package : libmagic1_1:5.25-2ubuntu1.1
 - Fixed package : libmagic1_1:5.25-2ubuntu1.4

133144 - Ubuntu 16.04 LTS / 18.04 LTS : libbsd vulnerabilities (USN-4243-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4243-1 advisory.

It was discovered that libbsd incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 ESM. (CVE-2016-2090)

It was discovered that libbsd incorrectly handled certain strings. An attacker could possibly use this issue to access sensitive information. (CVE-2019-20367)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4243-1>

Solution

Update the affected libbsd-dev, libbsd0 and / or libbsd0-udeb 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-2016-2090
CVE	CVE-2019-20367
XREF	USN:4243-1

Plugin Information

Published: 2020/01/21, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libbsd0_0.8.2-1
- Fixed package : libbsd0_0.8.2-1ubuntu0.1

131016 - Ubuntu 16.04 LTS / 18.04 LTS : libjpeg-turbo vulnerabilities (USN-4190-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4190-1 advisory.

It was discovered that libjpeg-turbo incorrectly handled certain BMP images. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-14498)

It was discovered that libjpeg-turbo incorrectly handled certain JPEG images. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 19.04. (CVE-2018-19664)

It was discovered that libjpeg-turbo incorrectly handled certain BMP images. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 19.04. (CVE-2018-20330)

It was discovered that libjpeg-turbo incorrectly handled certain JPEG images. An attacker could possibly cause a denial of service or execute arbitrary code. (CVE-2019-2201)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4190-1>

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-2018-14498
CVE	CVE-2018-19664
CVE	CVE-2018-20330
CVE	CVE-2019-2201
XREF	USN:4190-1

Plugin Information

Published: 2019/11/14, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libjpeg-turbo8_1.4.2-0ubuntu3.1
- Fixed package : libjpeg-turbo8_1.4.2-0ubuntu3.3

214886 - Ubuntu 16.04 LTS / 18.04 LTS : libndp vulnerability (USN-7248-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7248-1 advisory.

It was discovered that libndp incorrectly handled certain malformed IPv6 router advertisement packets. A local attacker could possibly use this issue to cause NetworkManager to crash, resulting in a denial of service, or the execution of 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-7248-1>

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:7248-1

Plugin Information

Published: 2025/02/03, Modified: 2025/02/03

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 : libndp0_1.4-2ubuntu0.16.04.1
- Fixed package : libndp0_1.4-2ubuntu0.16.04.1+esm1

125624 - Ubuntu 16.04 LTS / 18.04 LTS : libseccomp vulnerability (USN-4001-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4001-1 advisory.

Jann Horn discovered that libseccomp did not correctly generate 64-bit syscall argument comparisons with arithmetic operators (LT, GT, LE, GE). An attacker could use this to bypass intended access restrictions for argument-filtered system calls.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4001-1>

Solution

Update the affected libseccomp-dev, libseccomp2 and / or seccomp 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-2019-9893
XREF	USN:4001-1

Plugin Information

Published: 2019/05/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libseccomp2_2.3.1-2.1ubuntu2~16.04.1
- Fixed package : libseccomp2_2.4.1-0ubuntu0.16.04.2

238438 - Ubuntu 16.04 LTS / 18.04 LTS : libsoup vulnerabilities (USN-7565-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7565-1 advisory.

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. This issue only affected Ubuntu 16.04 LTS. (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. This issue only affected Ubuntu 16.04 LTS. (CVE-2024-52532)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7565-1>

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 (CVSS:2.0/AV:N/AC:L/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

5.8 (CVSS:2.0/E:U/RL:OF/RC:C)

References

CVE	CVE-2024-52531
CVE	CVE-2024-52532
CVE	CVE-2025-2784
CVE	CVE-2025-32050
CVE	CVE-2025-32052
CVE	CVE-2025-32053
XREF	USN:7565-1

Plugin Information

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

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.

- Installed package : gir1.2-soup-2.4_2.52.2-1ubuntu0.3
- Fixed package : gir1.2-soup-2.4_2.52.2-1ubuntu0.3+esm4
- Installed package : libsshd2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsshd2.4-1_2.52.2-1ubuntu0.3+esm4
- Installed package : libsshd2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsshd2.4-1_2.52.2-1ubuntu0.3+esm4

132014 - Ubuntu 16.04 LTS / 18.04 LTS : libssh vulnerability (USN-4219-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4219-1 advisory.

It was discovered that libssh incorrectly handled certain scp commands. If a user or automated system were tricked into using a specially-crafted scp command, a remote attacker could execute arbitrary commands on the 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-4219-1>

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: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-2019-14889
XREF	USN:4219-1
XREF	IAVA:2020-A-0203

Plugin Information

Published: 2019/12/12, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libssh-4_0.6.3-4.3ubuntu0.2
- Fixed package : libssh-4_0.6.3-4.3ubuntu0.5

131314 - Ubuntu 16.04 LTS / 18.04 LTS : libvpx vulnerabilities (USN-4199-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4199-1 advisory.

It was discovered that libvpx did not properly handle certain malformed WebM media files. If an application using libvpx opened a specially crafted WebM 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-4199-1>

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

References

CVE	CVE-2017-13194
CVE	CVE-2019-2126
CVE	CVE-2019-9232
CVE	CVE-2019-9325
CVE	CVE-2019-9371
CVE	CVE-2019-9433
XREF	USN:4199-1

Plugin Information

Published: 2019/11/26, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libvpx3_1.5.0-2ubuntu1
- Fixed package : libvpx3_1.5.0-2ubuntu1.1

126257 - Ubuntu 16.04 LTS / 18.04 LTS : policykit-desktop-privileges update (USN-4037-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4037-1 advisory.

The policykit-desktop-privileges Startup Disk Creator policy allowed administrative users to overwrite disks. As a security improvement, this operation now requires 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-4037-1>

Solution

Update the affected policykit-desktop-privileges package.

Risk Factor

High

References

XREF	USN:4037-1
------	------------

Plugin Information

Published: 2019/06/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : policykit-desktop-privileges_0.20
- Fixed package : policykit-desktop-privileges_0.20ubuntu16.04.1

126375 - Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4042-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4042-1 advisory.

It was discovered that poppler incorrectly handled certain files. If a user or automated system were tricked into opening a crafted PDF file, an 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-4042-1>

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-2017-9865
CVE	CVE-2018-18897
CVE	CVE-2018-20662
CVE	CVE-2019-10018
CVE	CVE-2019-10019
CVE	CVE-2019-10021
CVE	CVE-2019-10023
CVE	CVE-2019-10872
CVE	CVE-2019-10873
CVE	CVE-2019-12293
CVE	CVE-2019-9200
CVE	CVE-2019-9631
CVE	CVE-2019-9903
XREF	USN:4042-1

Plugin Information

Published: 2019/07/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.14
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.14
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.14

133950 - Ubuntu 16.04 LTS / 18.04 LTS : ppp vulnerability (USN-4288-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4288-1 advisory.

It was discovered that ppp incorrectly handled certain rhostring values. A remote attacker could use this issue to cause ppp 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-4288-1>

Solution

Update the affected ppp, ppp-dev and / or ppp-udeb 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-2020-8597
XREF	USN:4288-1
XREF	CEA-ID:CEA-2020-0025

Plugin Information

Published: 2020/02/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ppp_2.4.7-1+2ubuntu1.16.04.1
- Fixed package : ppp_2.4.7-1+2ubuntu1.16.04.2

134039 - Ubuntu 16.04 LTS / 18.04 LTS : rsync vulnerabilities (USN-4292-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4292-1 advisory.

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

(CVE-2016-9840, CVE-2016-9841)

It was discovered that rsync incorrectly handled vectors involving left shifts of negative integers in zlib. An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9842)

It was discovered that rsync incorrectly handled vectors involving big-endian CRC calculation in zlib. An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9843)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4292-1>

Solution

Update the affected rsync 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-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2016-9842
CVE	CVE-2016-9843
XREF	USN:4292-1

Plugin Information

Published: 2020/02/25, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : rsync_3.1.1-3ubuntu1.2
- Fixed package : rsync_3.1.1-3ubuntu1.3

133291 - Ubuntu 16.04 LTS / 18.04 LTS : tcpdump vulnerabilities (USN-4252-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4252-1 advisory.

Multiple security issues were discovered in tcpdump. A remote attacker could use these issues to cause tcpdump 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-4252-1>

Solution

Update the affected tcpdump 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

CVE	CVE-2017-16808
CVE	CVE-2018-10103
CVE	CVE-2018-10105
CVE	CVE-2018-14461
CVE	CVE-2018-14462
CVE	CVE-2018-14463
CVE	CVE-2018-14464
CVE	CVE-2018-14465
CVE	CVE-2018-14466
CVE	CVE-2018-14467
CVE	CVE-2018-14468
CVE	CVE-2018-14469
CVE	CVE-2018-14470
CVE	CVE-2018-14879
CVE	CVE-2018-14880
CVE	CVE-2018-14881
CVE	CVE-2018-14882
CVE	CVE-2018-16227
CVE	CVE-2018-16228
CVE	CVE-2018-16229
CVE	CVE-2018-16230
CVE	CVE-2018-16300
CVE	CVE-2018-16451
CVE	CVE-2018-16452
CVE	CVE-2018-19519
CVE	CVE-2019-1010220
CVE	CVE-2019-15166
CVE	CVE-2019-15167
XREF	USN:4252-1

Plugin Information

Published: 2020/01/28, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : tcpdump_4.9.2-0ubuntu0.16.04.1
- Fixed package : tcpdump_4.9.3-0ubuntu0.16.04.1

126748 - Ubuntu 16.04 LTS : Bash vulnerability (USN-4058-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4058-1 advisory.

It was discovered that Bash incorrectly handled the restricted shell. An attacker could possibly use this issue to escape restrictions and execute any command.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4058-1>

Solution

Update the affected bash, bash-builtins and / or bash-static 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-2019-9924
XREF USN:4058-1

Plugin Information

Published: 2019/07/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bash_4.3-14ubuntu1.2
- Fixed package : bash_4.3-14ubuntu1.4

205642 - Ubuntu 16.04 LTS : Bind vulnerabilities (USN-6909-3)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6909-3 advisory.

USN-6909-1 fixed vulnerabilities in Bind. This update provides the corresponding updates for Ubuntu 16.04 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-6909-3>

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

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

CVSS v2.0 Base Score

7.8 (CVSS:3.0/A:U/C:N/I:N/R:N)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-1737
CVE	CVE-2024-1975
XREF	USN:6909-3
XREF	IAVA:2024-A-0442-S

Plugin Information

Published: 2024/08/15, Modified: 2025/01/30

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 : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm9

208229 - Ubuntu 16.04 LTS : CUPS vulnerability (USN-7041-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7041-3 advisory.

USN-7041-1 fixed a vulnerability in CUPS. This update provides the corresponding update for Ubuntu 16.04 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-7041-3>

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-2024-47175
XREF USN:7041-3

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/10/07, Modified: 2024/11/25

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm8
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm8
- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.11+esm8
- Installed package : libcurlcgi1_2.1.3-4ubuntu0.7
- Fixed package : libcurlcgi1_2.1.3-4ubuntu0.11+esm8
- Installed package : libcurlimage2_2.1.3-4ubuntu0.7
- Fixed package : libcurlimage2_2.1.3-4ubuntu0.11+esm8
- Installed package : libcurlsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsmime1_2.1.3-4ubuntu0.11+esm8
- Installed package : libcurlppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlppdc1_2.1.3-4ubuntu0.11+esm8

141923 - Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4599-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4599-2 advisory.

USN-4599-1 fixed vulnerabilities in Firefox. This update provides the corresponding updates for Ubuntu 16.04 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-4599-2>

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-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:4599-2

Plugin Information

Published: 2020/10/27, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_82.0+build2-0ubuntu0.16.04.5
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_82.0+build2-0ubuntu0.16.04.5

143127 - Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4637-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4637-2 advisory.

USN-4637-1 fixed vulnerabilities in Firefox. This update provides the corresponding updates for Ubuntu 16.04 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-4637-2>

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:4637-2

Plugin Information

Published: 2020/11/20, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_83.0+build2-0ubuntu0.16.04.3

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_83.0+build2-0ubuntu0.16.04.3

127791 - Ubuntu 16.04 LTS : GLib regression (USN-4049-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4049-3 advisory.

USN-4049-1 fixed a vulnerability in GLib. The update introduced a regression in Ubuntu 16.04 LTS causing a possibly memory leak. 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-4049-3>

Solution

Update the affected packages.

Risk Factor

High

References

XREF USN:4049-3

Plugin Information

Published: 2019/08/12, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.4
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.4
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.4

125142 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3981-2)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3981-2 advisory.

USN-3981-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 LTS for Ubuntu 16.04 LTS and for the Linux Azure kernel for Ubuntu 14.04 LTS.

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Giorgi Maisuradze, Dan Horea Lutas, Andrei Lutas, Volodymyr Pikhur, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Moritz Lipp, Michael Schwarz, and Daniel Gruss discovered that memory previously stored in microarchitectural fill buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12130)

Brandon Falk, Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that memory previously stored in microarchitectural load ports of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12127)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Marina Minkin, Daniel Moghim, Moritz Lipp, Michael Schwarz, Jo Van Bulck, Daniel Genkin, Daniel Gruss, Berk Sunar, Frank Piessens, and Yuval Yarom discovered that memory previously stored in microarchitectural store buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12126)

Vasily Averin and Evgenii Shatokhin discovered that a use-after-free vulnerability existed in the NFS41+ subsystem when multiple network namespaces are in use. A local attacker in a container could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-16884)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Volodrmry Pikhur, Moritz Lipp, Michael Schwarz, Daniel Gruss, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that uncacheable memory previously stored in microarchitectural

buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11091)

Matteo Croce, Natale Vinto, and Andrea Spagnolo discovered that the cgroups subsystem of the Linux kernel did not properly account for SCTP socket buffers. A local attacker could use this to cause a denial of service (system crash). (CVE-2019-3874)

Alex Williamson discovered that the vfio subsystem of the Linux kernel did not properly limit DMA mappings. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2019-3882)

Hugues Anguelkov discovered that the Broadcom Wifi driver in the Linux kernel contained a heap buffer overflow. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-9500)

Hugues Anguelkov discovered that the Broadcom Wifi driver in the Linux kernel did not properly prevent remote firmware events from being processed for USB Wifi devices. A physically proximate attacker could use this to send firmware events to the device. (CVE-2019-9503)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3981-2>

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (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-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2018-16884
CVE	CVE-2019-11091
CVE	CVE-2019-3874
CVE	CVE-2019-3882
CVE	CVE-2019-9500
CVE	CVE-2019-9503
XREF	USN:3981-2
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/05/15, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-50-generic for this advisory.

126949 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4068-2)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4068-2 advisory.

USN-4068-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 for Ubuntu 16.04 LTS.

Adam Zabrocki discovered that the Intel i915 kernel mode graphics driver in the Linux kernel did not properly restrict mmap() ranges in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-11085)

It was discovered that a race condition leading to a use-after-free existed in the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel. The RDS protocol is disabled via blocklist by default in Ubuntu.

If enabled, a local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-11815)

It was discovered that the ext4 file system implementation in the Linux kernel did not properly zero out memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2019-11833)

It was discovered that the Bluetooth Human Interface Device Protocol (HIDP) implementation in the Linux kernel did not properly verify strings were NULL terminated in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2019-11884)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4068-2>

Solution

Update the affected kernel package.

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

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-2019-11085
CVE	CVE-2019-11815
CVE	CVE-2019-11833
CVE	CVE-2019-11884
XREF	USN:4068-2

Plugin Information

Published: 2019/07/23, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-55-generic for this advisory.

124679 - Ubuntu 16.04 LTS : Sudo vulnerabilities (USN-3968-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3968-1 advisory.

Florian Weimer discovered that Sudo incorrectly handled the noexec restriction when used with certain applications. A local attacker could possibly use this issue to bypass configured restrictions and execute arbitrary commands. (CVE-2016-7076)

It was discovered that Sudo did not properly parse the contents of /proc/[pid]/stat when attempting to determine its controlling tty. A local attacker in some configurations could possibly use this to overwrite any file on the filesystem, bypassing intended permissions. (CVE-2017-1000368)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3968-1>

Solution

Update the affected sudo and / or sudo-ldap packages.

Risk Factor

High

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

7.1 (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-2016-7076
CVE	CVE-2017-1000368
XREF	USN:3968-1

Plugin Information

Published: 2019/05/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : sudo_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.6

135896 - Ubuntu 16.04 LTS : Thunderbird vulnerabilities (USN-4335-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4335-1 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, bypass same-origin restrictions, conduct cross-site scripting (XSS) attacks, or execute arbitrary code. (CVE-2019-11757, CVE-2019-11758, CVE-2019-11759, CVE-2019-11760, CVE-2019-11761, CVE-2019-11762, CVE-2019-11763, CVE-2019-11764, CVE-2019-17005, CVE-2019-17008, CVE-2019-17010, CVE-2019-17011, CVE-2019-17012, CVE-2019-17016, CVE-2019-17017, CVE-2019-17022, CVE-2019-17024, CVE-2019-17026, CVE-2019-20503, CVE-2020-6798, CVE-2020-6800, CVE-2020-6805, CVE-2020-6806, CVE-2020-6807, CVE-2020-6812, CVE-2020-6814, CVE-2020-6819, CVE-2020-6820, CVE-2020-6821, CVE-2020-6825)

It was discovered that NSS incorrectly handled certain memory operations. A remote attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2019-11745)

It was discovered that a specially crafted S/MIME message with an inner encryption layer could be displayed as having a valid signature in some circumstances, even if the signer had no access to the encrypted message. An attacker could potentially exploit this to spoof the message author. (CVE-2019-11755)

A heap overflow was discovered in the expat library in Thunderbird. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2019-15903)

It was discovered that Message ID calculation was based on uninitialized data. An attacker could potentially exploit this to obtain sensitive information. (CVE-2020-6792)

Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2020-6793, CVE-2020-6795, CVE-2020-6822)

It was discovered that if a user saved passwords before Thunderbird 60 and then later set a primary password, an unencrypted copy of these passwords would still be accessible. A local user could exploit this to obtain sensitive information. (CVE-2020-6794)

It was discovered that the Devtools Copy as cURL feature did not fully escape website-controlled data. If a user were tricked in to using the Copy as cURL feature to copy and paste a command with specially crafted data in to a terminal, an attacker could potentially exploit this to execute arbitrary commands via command injection. (CVE-2020-6811)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4335-1>

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

9.4 (CVSS:3.0/E:H/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

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

References

CVE	CVE-2019-11745
CVE	CVE-2019-11755
CVE	CVE-2019-11757
CVE	CVE-2019-11758
CVE	CVE-2019-11759
CVE	CVE-2019-11760
CVE	CVE-2019-11761
CVE	CVE-2019-11762
CVE	CVE-2019-11763
CVE	CVE-2019-11764
CVE	CVE-2019-15903
CVE	CVE-2019-17005
CVE	CVE-2019-17008
CVE	CVE-2019-17010
CVE	CVE-2019-17011
CVE	CVE-2019-17012
CVE	CVE-2019-17016
CVE	CVE-2019-17017
CVE	CVE-2019-17022
CVE	CVE-2019-17024
CVE	CVE-2019-17026

CVE	CVE-2019-20503
CVE	CVE-2020-6792
CVE	CVE-2020-6793
CVE	CVE-2020-6794
CVE	CVE-2020-6795
CVE	CVE-2020-6798
CVE	CVE-2020-6800
CVE	CVE-2020-6805
CVE	CVE-2020-6806
CVE	CVE-2020-6807
CVE	CVE-2020-6811
CVE	CVE-2020-6812
CVE	CVE-2020-6814
CVE	CVE-2020-6819
CVE	CVE-2020-6820
CVE	CVE-2020-6821
CVE	CVE-2020-6822
CVE	CVE-2020-6825
XREF	USN:4335-1
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2020-0032
XREF	CEA-ID:CEA-2020-0007

Plugin Information

Published: 2020/04/22, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : thunderbird_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird_1:68.7.0+build1-0ubuntu0.16.04.2

- Installed package : thunderbird-gnome-support_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-gnome-support_1:68.7.0+build1-0ubuntu0.16.04.2

- Installed package : thunderbird-locale-en_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en_1:68.7.0+build1-0ubuntu0.16.04.2

- Installed package : thunderbird-locale-en-us_1:60.5.1+build2-0ubuntu0.16.04.1
- Fixed package : thunderbird-locale-en-us_1:68.7.0+build1-0ubuntu0.16.04.2
```

208231 - Ubuntu 16.04 LTS : cups-filters vulnerability (USN-7043-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7043-3 advisory.

USN-7043-1 fixed a vulnerability in cups-filters. This update provides the corresponding update for Ubuntu 16.04 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-7043-3>

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.9 (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-2024-47176
XREF	USN:7043-3

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/10/07, Modified: 2024/11/25

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 : cups-browsed_1.8.3-2ubuntu3.4
- Fixed package : cups-browsed_1.8.3-2ubuntu3.5+esm2
- Installed package : cups-filters_1.8.3-2ubuntu3.4
- Fixed package : cups-filters_1.8.3-2ubuntu3.5+esm2
- Installed package : cups-filters-core-drivers_1.8.3-2ubuntu3.4
- Fixed package : cups-filters-core-drivers_1.8.3-2ubuntu3.5+esm2
- Installed package : libcupsfilters1_1.8.3-2ubuntu3.4
- Fixed package : libcupsfilters1_1.8.3-2ubuntu3.5+esm2
- Installed package : libfontembed1_1.8.3-2ubuntu3.4
- Fixed package : libfontembed1_1.8.3-2ubuntu3.5+esm2

145464 - Ubuntu 16.04 LTS : libsndfile vulnerabilities (USN-4704-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4704-1 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. (CVE-2017-12562)

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. This issue only affected Ubuntu 14.04 ESM. (CVE-2017-14245, CVE-2017-14246, CVE-2017-14634, CVE-2017-16942, CVE-2017-6892, CVE-2018-13139, CVE-2018-19432, CVE-2018-19661, CVE-2018-19662, CVE-2018-19758, CVE-2019-3832)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4704-1>

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs 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

BID	105996
BID	107572
BID	107580
CVE	CVE-2017-6892
CVE	CVE-2017-12562
CVE	CVE-2017-14245
CVE	CVE-2017-14246
CVE	CVE-2017-14634
CVE	CVE-2017-16942
CVE	CVE-2018-13139
CVE	CVE-2018-19432
CVE	CVE-2018-19661
CVE	CVE-2018-19662
CVE	CVE-2018-19758
CVE	CVE-2019-3832
XREF	USN:4704-1

Plugin Information

Published: 2021/01/27, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.3

192115 - Ubuntu 16.04 LTS : python-cryptography vulnerability (USN-6673-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6673-2 advisory.

USN-6673-1 provided a security update for python-cryptography. This update provides the corresponding update for Ubuntu 16.04 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-6673-2>

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
XREF	USN:6673-2

Plugin Information

Published: 2024/03/14, Modified: 2024/10/29

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-cryptography_1.2.3-1ubuntu0.2
- Fixed package : python3-cryptography_1.2.3-1ubuntu0.3+esm1

133204 - Ubuntu 16.04 LTS : zlib vulnerabilities (USN-4246-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4246-1 advisory.

It was discovered that zlib incorrectly handled pointer arithmetic. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9840, CVE-2016-9841)

It was discovered that zlib incorrectly handled vectors involving left shifts of negative integers. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9842)

It was discovered that zlib incorrectly handled vectors involving big-endian CRC calculation. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2016-9843)

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

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

See Also

<https://ubuntu.com/security/notices/USN-4246-1>

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-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2016-9842
CVE	CVE-2016-9843
XREF	USN:4246-1

Plugin Information

Published: 2020/01/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.1
- Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

Solution

Upgrade to JQuery version 3.5.0 or later.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

XREF

CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/80/www

URL : <http://10.84.42.93/assets/js/jquery.min.js>
Installed version : 1.11.3
Fixed version : 3.5.0

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

Solution

Upgrade to JQuery version 3.5.0 or later.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/8000/www

URL : <http://10.84.42.93:8000/app/site/themes/common/js/jquery.min.js>
Installed version : 1.12.4
Fixed version : 3.5.0

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
```

198044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : jinja2 vulnerability (USN-6787-1)

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-6787-1 advisory.

It was discovered that Jinja2 incorrectly handled certain HTML attributes that were accepted by the `xmlattr` filter. An attacker could use this issue to inject arbitrary HTML attribute keys and values to potentially execute a cross-site scripting (XSS) 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-6787-1>

Solution

Update the affected `python-jinja2` and / or `python3-jinja2` 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-2024-34064
XREF	USN:6787-1

Plugin Information

Published: 2024/05/28, 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.

- Installed package : python3-jinja2_2.8-1
- Fixed package : python3-jinja2_2.8-1ubuntu0.1+esm3

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm16

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

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 : libcdio-cdda1_0.83-4.2ubuntu1
- Fixed package : libcdio-cdda1_0.83-4.2ubuntu1+esm3
- Installed package : libcdio-paranoia1_0.83-4.2ubuntu1
- Fixed package : libcdio-paranoia1_0.83-4.2ubuntu1+esm3
- Installed package : libcdio13_0.83-4.2ubuntu1
- Fixed package : libcdio13_0.83-4.2ubuntu1+esm3

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:O/RC:C)

References

CVE
XREF

CVE-2024-28219
USN:6744-1

Plugin Information

Published: 2024/04/23, 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.

- Installed package : python3-pil_3.1.2-0ubuntu1.1
- Fixed package : python3-pil_3.1.2-0ubuntu1.6+esm2

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
XREF USN:6640-1

Plugin Information

Published: 2024/02/15, 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.

- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm4

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm4

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_2.9.1-3ubuntu0.1
- Fixed package : python3-requests_2.9.1-3ubuntu0.1+esm2

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

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 : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm10

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-2025-3576
XREF USN:7542-1

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 : krb5-locales_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2+esm7
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2+esm7
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2+esm7
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2+esm7
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2+esm7

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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm24
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm24
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm24
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm24

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-2024-5290
USN:6945-1

Plugin Information

Published: 2024/08/06, Modified: 2024/09/18

Plugin Output

tcp/0

- Installed package : wpasupplicant_2.4-0ubuntu6.3
- Fixed package : wpasupplicant_2.4-0ubuntu6.8+esm1

235360 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Python vulnerabilities (USN-7488-1)

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 / 24.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7488-1 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. This issue only affected python 2.7 and python3.4 on Ubuntu 14.04 LTS; python2.7 on Ubuntu 16.04 LTS; python2.7, python3.6, python3.7, and python3.8 on Ubuntu 18.04 LTS; python2.7 and python3.9 on Ubuntu 20.04 LTS; and python2.7 and python3.11 on Ubuntu 22.04 LTS. (CVE-2024-11168)

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 excessive resources, leading to a denial of service. This issue only affected python3.4 on Ubuntu 14.04 LTS; python3.6, python3.7, and python3.8 on Ubuntu 18.04 LTS; python3.9 on Ubuntu 20.04 LTS; and python3.11 on Ubuntu 22.04 LTS. (CVE-2024-6232)

It was discovered that Python incorrectly handled quoted 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. This issue only affected python3.4 on Ubuntu 14.04 LTS; python3.6, python3.7, and python3.8 on Ubuntu 18.04 LTS; python3.9 on Ubuntu 20.04 LTS; python3.11 on Ubuntu 22.04 LTS; and python3.13 on Ubuntu 24.10. (CVE-2024-9287)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7488-1>

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/VA: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

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-2024-6232
CVE	CVE-2024-9287
CVE	CVE-2024-11168
XREF	USN:7488-1

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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm15
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm15
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm15
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm15
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm15

183603 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-3919-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3919-1 advisory.

Two security issues were discovered in the JavaScript engine in Firefox. If a user were tricked into opening a specially crafted website, an attacker could exploit this by causing a denial of service, or executing 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-3919-1>

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

8.4 (CVSS:3.0/E:H/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

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

STIG Severity

I

References

CVE	CVE-2019-9810
CVE	CVE-2019-9813
XREF	IAVA:2019-A-0089-S
XREF	USN:3919-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_66.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_66.0.1+build1-0ubuntu0.16.04.1

123075 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-3915-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3915-1 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3915-1>

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: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

4.3 (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-2019-3835
CVE	CVE-2019-3838
XREF	USN:3915-1

Plugin Information

Published: 2019/03/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.8`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.8`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.8`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.8`

125136 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Intel Microcode update (USN-3977-1)

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 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3977-1 advisory.

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Giorgi Maisuradze, Dan Horea Lutas, Andrei Lutas, Volodymyr Pikhur, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Moritz Lipp, Michael Schwarz, and Daniel Gruss discovered that memory previously stored in microarchitectural fill buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12130)

Brandon Falk, Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that memory previously stored in microarchitectural load ports of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12127)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Marina Minkin, Daniel Moghimi, Moritz Lipp, Michael Schwarz, Jo Van Bulck, Daniel Genkin, Daniel Gruss, Berk Sunar, Frank Piessens, and Yuval Yarom discovered that memory previously stored in microarchitectural store buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12126)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Volodrmir Pikhur, Moritz Lipp, Michael Schwarz, Daniel Gruss, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that uncacheable memory previously stored in microarchitectural buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11091)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3977-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

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

5.1 (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-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2019-11091
XREF	USN:3977-1
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/05/15, Modified: 2025/03/05

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20190514.0ubuntu0.16.04.1
```

126095 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Intel Microcode update (USN-3977-3)

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 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3977-3 advisory.

USN-3977-1 and USN-3977-2 provided mitigations for Microarchitectural Data Sampling (MDS) vulnerabilities in Intel Microcode for a large number of Intel processor families. This update provides the corresponding updated microcode mitigations for the Intel Sandy Bridge processor family

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Giorgi Maisuradze, Dan Horea Lutas, Andrei Lutas, Volodymyr Pikhur, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Moritz Lipp, Michael Schwarz, and Daniel Gruss discovered that memory previously stored in microarchitectural fill buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12130)

Brandon Falk, Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that memory previously stored in microarchitectural load ports of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12127)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Marina Minkin, Daniel Moghimi, Moritz Lipp, Michael Schwarz, Jo Van Bulck, Daniel Genkin, Daniel Gruss, Berk Sunar, Frank Piessens, and Yuval Yarom discovered that memory previously stored in microarchitectural store buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12126)

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Volodrmry Pikhur, Moritz Lipp, Michael Schwarz, Daniel Gruss, Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that uncacheable memory previously stored in microarchitectural buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11091)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3977-3>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

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

5.1 (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-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2019-11091
XREF	USN:3977-3
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/06/21, Modified: 2025/03/03

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20190618.0ubuntu0.16.04.1

122811 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : LibTIFF vulnerabilities (USN-3906-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3906-1 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-3906-1>

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-2018-10779
CVE	CVE-2018-12900
CVE	CVE-2018-17000
CVE	CVE-2018-19210
CVE	CVE-2019-6128
CVE	CVE-2019-7663
XREF	USN:3906-1

Plugin Information

Published: 2019/03/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.6

193593 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6740-1)

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 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6740-1 advisory.

Wei Chen discovered that a race condition existed in the TIPC protocol implementation in the Linux kernel, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1382)

It was discovered that the virtio network implementation in the Linux kernel did not properly handle file references in the host, 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 (kernel memory). (CVE-2023-1838)

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)

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)

shanzhulig discovered that the DRM subsystem in the Linux kernel contained a race condition when performing certain operation while handling driver 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-2023-51043)

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 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)

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)

It was discovered that the SCTP protocol implementation in the Linux kernel contained a race condition when handling lock acquisition in certain situations. A local attacker could possibly use this to cause a denial of service (kernel deadlock). (CVE-2024-0639)

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;
- EDAC drivers;
- Media drivers;
- JFS file system; (CVE-2023-52603, CVE-2023-52464, CVE-2023-52600, CVE-2023-52445, CVE-2023-52451)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6740-1>

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-2023-1838
CVE	CVE-2023-1998
CVE	CVE-2023-6915
CVE	CVE-2023-24023
CVE	CVE-2023-51043
CVE	CVE-2023-51779
CVE	CVE-2023-52429
CVE	CVE-2023-52445
CVE	CVE-2023-52451
CVE	CVE-2023-52464
CVE	CVE-2023-52600
CVE	CVE-2023-52603
CVE	CVE-2024-0639
CVE	CVE-2024-23851
XREF	USN:6740-1

Plugin Information

Published: 2024/04/19, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-224-generic for this advisory.

234106 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7428-1)

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 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7428-1 advisory.

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-2022-23041)

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:

- HID subsystem;
- Network drivers;
- Mellanox network drivers;
- SCSI subsystem;
- SuperH / SH-Mobile drivers;
- File systems infrastructure;
- Ext4 file system;
- JFS file system;
- IP tunnels definitions;
- Network namespace;
- BPF subsystem;
- Networking core;
- HSR network protocol;
- IPv4 networking;

- IPv6 networking;

- Network traffic control; (CVE-2024-56615, CVE-2024-56600, CVE-2025-21700, CVE-2024-56658, CVE-2024-35960, CVE-2024-50265, CVE-2025-21702, CVE-2024-53227, CVE-2024-53165, CVE-2024-50167, CVE-2024-26863, CVE-2024-35973, CVE-2024-46826, CVE-2021-47119, CVE-2024-50302, CVE-2024-49952, CVE-2021-47101, CVE-2024-49948, CVE-2024-56595)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7428-1>

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-47101
CVE	CVE-2021-47119
CVE	CVE-2022-23041
CVE	CVE-2024-26863
CVE	CVE-2024-35960
CVE	CVE-2024-35973
CVE	CVE-2024-46826
CVE	CVE-2024-49948
CVE	CVE-2024-49952
CVE	CVE-2024-50167
CVE	CVE-2024-50265
CVE	CVE-2024-50302
CVE	CVE-2024-53165
CVE	CVE-2024-53227
CVE	CVE-2024-56595
CVE	CVE-2024-56600
CVE	CVE-2024-56615
CVE	CVE-2024-56658
CVE	CVE-2025-21700
CVE	CVE-2025-21702
XREF	CISA-KNOWN-EXPLOITED:2025/03/25
XREF	USN:7428-1

Plugin Information

Published: 2025/04/09, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-236-generic for this advisory.

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 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7627-1 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:

- PowerPC architecture;
- Block layer subsystem;
- ACPI drivers;
- NILFS2 file system;
- File systems infrastructure;
- Memory management;
- Network traffic control;
- USB sound devices; (CVE-2025-37932, CVE-2024-53197, CVE-2024-50116, CVE-2021-47379, CVE-2024-49958, CVE-2022-49179, CVE-2024-46787, CVE-2024-41070, CVE-2025-38000, CVE-2024-56662, CVE-2022-49176, CVE-2025-37798)

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

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

See Also

<https://ubuntu.com/security/notices/USN-7627-1>

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-2021-47379
CVE	CVE-2022-49176
CVE	CVE-2022-49179
CVE	CVE-2024-41070
CVE	CVE-2024-46787
CVE	CVE-2024-49958
CVE	CVE-2024-50116
CVE	CVE-2024-53197
CVE	CVE-2024-56662
CVE	CVE-2025-37798
CVE	CVE-2025-37932
CVE	CVE-2025-38000
XREF	CISA-KNOWN-EXPLOITED:2025/04/30
XREF	USN:7627-1

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-239-generic for this advisory.

122499 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : NSS vulnerability (USN-3898-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3898-1 advisory.

Hanno Bck and Damian Poddebski discovered that NSS incorrectly handled certain CMS functions. A remote attacker could possibly use this issue to cause NSS 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-3898-1>

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-2018-18508
XREF	USN:3898-1

Plugin Information

Published: 2019/02/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.5
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.5

192577 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6588-2 advisory.

USN-6588-1 fixed a vulnerability in PAM. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6588-2>

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:6588-2

Plugin Information

Published: 2024/03/26, Modified: 2024/10/29

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 : libpam-modules_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm5
- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm5
- Installed package : libpam-runtime_1.1.8-3.2ubuntu2.1
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm5
- Installed package : libpam0g_1.1.8-3.2ubuntu2.1
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm5

123750 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PolicyKit vulnerability (USN-3934-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3934-1 advisory.

It was discovered that PolicyKit incorrectly relied on the fork() system call in the Linux kernel being atomic. A local attacker could possibly use this issue to gain access to services that have cached authorizations.

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

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

See Also

<https://ubuntu.com/security/notices/USN-3934-1>

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

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-2019-6133
XREF	USN:3934-1

Plugin Information

Published: 2019/04/04, Modified: 2025/03/12

Plugin Output

tcp/0

```
- Installed package : libpolkit-agent-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-agent-1-0_0.105-14.1ubuntu0.5

- Installed package : libpolkit-backend-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-backend-1-0_0.105-14.1ubuntu0.5

- Installed package : libpolkit-gobject-1-0_0.105-14.1ubuntu0.4
- Fixed package : libpolkit-gobject-1-0_0.105-14.1ubuntu0.5

- Installed package : policykit-1_0.105-14.1ubuntu0.4
- Fixed package : policykit-1_0.105-14.1ubuntu0.5
```

183594 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : poppler vulnerability (USN-3905-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3905-1 advisory.

It was discovered that poppler incorrectly handled certain PDF 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-3905-1>

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-2019-9200
XREF	USN:3905-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.13
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.13
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.13

123077 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : snapd vulnerability (USN-3917-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3917-1 advisory.

The snapd default seccomp filter for strict mode snaps blocks the use of the ioctl() system call when used with TIOCSTI as the second argument to the system call. Jann Horn discovered that this restriction could be circumvented on 64 bit architectures. A malicious snap could exploit this to bypass intended access restrictions to insert characters into the terminal's input queue. On Ubuntu, snapd typically will have already automatically refreshed itself to snapd 2.37.4 which is unaffected.

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

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

See Also

<https://ubuntu.com/security/notices/USN-3917-1>

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)

References

CVE
XREF
CVE-2019-7303
USN:3917-1

Plugin Information

Published: 2019/03/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.37.4ubuntu0.1

- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.37.4ubuntu0.1

123930 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : systemd vulnerability (USN-3938-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3938-1 advisory.

Jann Horn discovered that pam_systemd created logind sessions using some parameters from the environment. A local attacker could exploit this in order to spoof the active session and gain additional PolicyKit 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-3938-1>

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-2019-3842
XREF	USN:3938-1

Plugin Information

Published: 2019/04/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpam-systemd_229-4ubuntu21.16
- Fixed package : libpam-systemd_229-4ubuntu21.21
- Installed package : libsystemd0_229-4ubuntu21.16
- Fixed package : libsystemd0_229-4ubuntu21.21
- Installed package : libudev1_229-4ubuntu21.16
- Fixed package : libudev1_229-4ubuntu21.21
- Installed package : systemd_229-4ubuntu21.16
- Fixed package : systemd_229-4ubuntu21.21
- Installed package : systemd-sysv_229-4ubuntu21.16
- Fixed package : systemd-sysv_229-4ubuntu21.21
- Installed package : udev_229-4ubuntu21.16
- Fixed package : udev_229-4ubuntu21.21

123999 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : wpa_supplicant and hostapd vulnerabilities (USN-3944-1)**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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3944-1 advisory.

It was discovered that wpa_supplicant and hostapd were vulnerable to a side channel attack against EAP- pwd. A remote attacker could possibly use this issue to recover certain passwords. (CVE-2019-9495)

Mathy Vanhoef discovered that wpa_supplicant and hostapd incorrectly validated received scalar and element values in EAP-pwd-Commit messages. A remote attacker could possibly use this issue to perform a reflection attack and authenticate without the appropriate password. (CVE-2019-9497, CVE-2019-9498, CVE-2019-9499)

It was discovered that hostapd incorrectly handled obtaining random numbers. In rare cases where the urandom device isn't available, it would fall back to using a low-quality PRNG. This issue only affected Ubuntu 14.04 LTS and Ubuntu 16.04 LTS. (CVE-2016-10743)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3944-1>

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-2016-10743
CVE	CVE-2019-9495
CVE	CVE-2019-9497
CVE	CVE-2019-9498
CVE	CVE-2019-9499
XREF	USN:3944-1

Plugin Information

Published: 2019/04/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : wpasupplicant_2.4-0ubuntu6.3
- Fixed package : wpasupplicant_2.4-0ubuntu6.4

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-4032
CVE	CVE-2024-9287
CVE	CVE-2024-11168
CVE	CVE-2025-0938
XREF	USN:7348-1

Plugin Information

Published: 2025/03/12, Modified: 2025/03/12

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 : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm16
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm16
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm16
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm16
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm16

209023 - Ubuntu 14.04 LTS / 16.04 LTS : ImageMagick vulnerabilities (USN-7068-1)

Synopsis

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

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7068-1 advisory.

It was discovered that ImageMagick incorrectly handled certain

malformed image files. If a user or automated system using ImageMagick were tricked into processing a specially crafted file, an attacker could exploit this to cause a denial of service or affect the reliability of the system. The vulnerabilities included memory leaks, buffer overflows, and improper handling of pixel data.

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

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

See Also

<https://ubuntu.com/security/notices/USN-7068-1>

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-2019-7397
CVE	CVE-2019-7398
CVE	CVE-2019-9956
CVE	CVE-2020-19667
CVE	CVE-2020-25664
CVE	CVE-2020-25665
CVE	CVE-2020-25666
CVE	CVE-2020-25674
CVE	CVE-2020-25676
CVE	CVE-2020-27560
CVE	CVE-2020-27750
CVE	CVE-2020-27753
CVE	CVE-2020-27754
CVE	CVE-2020-27755
CVE	CVE-2020-27758
CVE	CVE-2020-27759
CVE	CVE-2020-27760
CVE	CVE-2020-27761
CVE	CVE-2020-27762
CVE	CVE-2020-27763
CVE	CVE-2020-27764
CVE	CVE-2020-27765
CVE	CVE-2020-27766
CVE	CVE-2020-27767
CVE	CVE-2020-27768
CVE	CVE-2020-27769
CVE	CVE-2020-27770
CVE	CVE-2020-27771
CVE	CVE-2020-27772
CVE	CVE-2020-27773
CVE	CVE-2020-27774
CVE	CVE-2020-27775
CVE	CVE-2020-27776
XREF	IAVB:2019-B-0013-S
XREF	IAVB:2019-B-0032-S
XREF	IAVB:2020-B-0042-S
XREF	IAVB:2020-B-0076-S
XREF	USN:7068-1

Plugin Information

Published: 2024/10/15, Modified: 2024/10/15

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 : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm11
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm11
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm11
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm11
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13

- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm11
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm11

122647 - Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3901-2)

Synopsis

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

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3901-2 advisory.

USN-3901-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 LTS for Ubuntu 16.04 LTS.

Jann Horn discovered that the userfaultd implementation in the Linux kernel did not properly restrict access to certain ioctl. A local attacker could use this possibly to modify files. (CVE-2018-18397)

It was discovered that the crypto subsystem of the Linux kernel leaked uninitialized memory to user space in some situations. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2018-19854)

Jann Horn discovered a race condition in the fork() system call in the Linux kernel. A local attacker could use this to gain access to services that cache authorizations. (CVE-2019-6133)

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

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

See Also

<https://ubuntu.com/security/notices/USN-3901-2>

Solution

Update the affected kernel package.

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

6.0 (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-2018-18397
CVE	CVE-2018-19854
CVE	CVE-2019-6133
XREF	USN:3901-2

Plugin Information

Published: 2019/03/06, Modified: 2025/03/20

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-46-generic for this advisory.

189915 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : ImageMagick vulnerability (USN-6621-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6621-1 advisory.

It was discovered that ImageMagick incorrectly handled certain values when processing BMP files. An attacker could exploit this 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-6621-1>

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)

STIG Severity

I

References

CVE	CVE-2023-5341
XREF	USN:6621-1
XREF	IAVB:2023-B-0077-S

Plugin Information

Published: 2024/02/01, 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.

- Installed package : `imagemagick_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick_8:6.8.9.9-7ubuntu5.16+esm10`
- Installed package : `imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm10`
- Installed package : `imagemagick-common_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm10`
- Installed package : `libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm10`
- Installed package : `libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm10`
- Installed package : `libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm10`

177934 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 ESM / 23.04 : ImageMagick vulnerabilities (USN-6200-1)

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 ESM / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6200-1 advisory.

It was discovered that ImageMagick incorrectly handled the -authenticate option for password-protected PDF files. An attacker could possibly use this issue to inject additional shell commands and perform arbitrary code execution. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-29599)

It was discovered that ImageMagick incorrectly handled certain values when processing PDF files. If a user or automated system using ImageMagick were tricked into opening a specially crafted PDF file, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-20224)

Zhang Xiaohui discovered that ImageMagick incorrectly handled certain values when processing image data.

If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service.

This issue only affected Ubuntu 20.04 LTS.

(CVE-2021-20241, CVE-2021-20243)

It was discovered that ImageMagick incorrectly handled certain values when processing visual effects based image files. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-20244, CVE-2021-20309)

It was discovered that ImageMagick incorrectly handled certain values when performing resampling operations. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-20246)

It was discovered that ImageMagick incorrectly handled certain values when processing thumbnail image data. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-20312)

It was discovered that ImageMagick incorrectly handled memory cleanup when performing certain cryptographic operations. Under certain conditions sensitive cryptographic information could be disclosed.

This issue only affected Ubuntu 20.04 LTS. (CVE-2021-20313)

It was discovered that ImageMagick did not use the correct rights when specifically excluded by a module policy. An attacker could use this issue to read and write certain restricted files. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-3912)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 20.04 LTS. (CVE-2022-28463, CVE-2022-32545, CVE-2022-32546, CVE-2022-32547)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2021-3610, CVE-2023-1906, CVE-2023-3428)

It was discovered that ImageMagick incorrectly handled certain values when processing specially crafted SVG files. By tricking a user into opening a specially crafted SVG file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-1289)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted tiff file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-3195)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. (CVE-2023-34151)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6200-1>

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 (CVSS:2.0/AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS:2.0/E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-29599
CVE	CVE-2021-3610
CVE	CVE-2021-20224
CVE	CVE-2021-20241
CVE	CVE-2021-20243
CVE	CVE-2021-20244
CVE	CVE-2021-20246
CVE	CVE-2021-20309
CVE	CVE-2021-20312
CVE	CVE-2021-20313
CVE	CVE-2021-39212
CVE	CVE-2022-28463
CVE	CVE-2022-32545
CVE	CVE-2022-32546
CVE	CVE-2022-32547
CVE	CVE-2023-1289
CVE	CVE-2023-1906
CVE	CVE-2023-3195
CVE	CVE-2023-3428
CVE	CVE-2023-34151
XREF	USN:6200-1
XREF	IAVB:2020-B-0076-S
XREF	IAVB:2021-B-0017-S
XREF	IAVB:2022-B-0032-S
XREF	IAVB:2023-B-0020-S
XREF	IAVB:2023-B-0038-S
XREF	IAVB:2022-B-0019-S
XREF	IAVB:2023-B-0046-S

Plugin Information

Published: 2023/07/04, 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.

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm8
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm8
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm8
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm8
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm8
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm8

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

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 : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3+esm3
- Installed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3+esm3
- Installed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3+esm3
- Installed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3+esm3

```
- Installed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3+esm3

- Installed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3+esm3

- Installed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3+esm3

- Installed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3+esm3

- Installed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3+esm3
```

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

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 : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3+esm3
```

```
- Installed package : bluez-cups_5.37-0ubuntu5.1
- Fixed package : bluez-cups_5.37-0ubuntu5.3+esm3

- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3+esm3

- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3+esm3
```

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 Gosen, 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/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-2023-23583
XREF	USN:6485-1

Plugin Information

Published: 2023/11/16, 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.

```
- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20231114.0ubuntu0.16.04.1+esm1
```

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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm22
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm22
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm22
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm22

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/V/I:H/V/A: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

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 : amd64-microcode_3.20180524.1~ubuntu0.16.04.2
- Fixed package : amd64-microcode_3.20191021.1+really3.20180524.1~ubuntu0.16.04.2+esm1

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

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_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm6`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm6`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm6`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm6`

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/RL: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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20230808.0ubuntu0.16.04.1+esm1

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	CVE-2023-1916
XREF	USN:6428-1

Plugin Information

Published: 2023/10/11, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm13

189537 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 : Jinja2 vulnerabilities (USN-6599-1)

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 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6599-1 advisory.

Yeting Li discovered that Jinja incorrectly handled certain regex. An 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 20.04 LTS. (CVE-2020-28493)

It was discovered that Jinja incorrectly handled certain HTML passed with xmllatter filter. An attacker could inject arbitrary HTML attributes keys and values potentially leading to XSS. (CVE-2024-22195)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6599-1>

Solution

Update the affected python-jinja2 and / or python3-jinja2 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

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

CVSS v3.0 Temporal Score

5.5 (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-2020-28493
CVE	CVE-2024-22195
XREF	USN:6599-1

Plugin Information

Published: 2024/01/25, 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.

- Installed package : python3-jinja2_2.8-1
- Fixed package : python3-jinja2_2.8-1ubuntu0.1+esm2

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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm19
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm19
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm19
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm19

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

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 : libelf1_0.165-3ubuntu1.1
- Fixed package : libelf1_0.165-3ubuntu1.2+esm1

181839 - Ubuntu 16.04 ESM / 18.04 ESM : AccountsService vulnerability (USN-6190-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6190-2 advisory.

USN-6190-1 fixed a vulnerability in AccountsService. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6190-2>

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:6190-2

Plugin Information

Published: 2023/09/25, Modified: 2024/10/29

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 : accountsservice_0.6.40-2ubuntu11.3
- Fixed package : accountsservice_0.6.40-2ubuntu11.6+esm1
- Installed package : libaccountsservice0_0.6.40-2ubuntu11.3
- Fixed package : libaccountsservice0_0.6.40-2ubuntu11.6+esm1

178778 - Ubuntu 16.04 ESM / 18.04 ESM : Avahi vulnerability (USN-6129-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6129-2 advisory.

USN-6129-1 fixed a vulnerability in Avahi. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6129-2>

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-2023-1981
XREF	USN:6129-2

Plugin Information

Published: 2023/07/25, Modified: 2024/10/29

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 : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3+esm2
- Installed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3+esm2

180472 - Ubuntu 16.04 ESM / 18.04 ESM : BusyBox vulnerabilities (USN-6335-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6335-1 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 execute arbitrary code. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-28831)

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 BusyBox to crash, resulting in a denial of service, or execute arbitrary code. (CVE-2022-48174)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6335-1>

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

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

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-2021-28831
CVE	CVE-2022-48174
XREF	USN:6335-1

Plugin Information

Published: 2023/09/04, 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.

- Installed package : busybox-initramfs_1:1.22.0-15ubuntu1
- Fixed package : busybox-initramfs_1:1.22.0-15ubuntu1.4+esm2
- Installed package : busybox-static_1:1.22.0-15ubuntu1
- Fixed package : busybox-static_1:1.22.0-15ubuntu1.4+esm2

178326 - Ubuntu 16.04 ESM / 18.04 ESM : CUPS vulnerability (USN-6184-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6184-2 advisory.

USN-6184-1 fixed a vulnerability in CUPS. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6184-2>

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:6184-2

Plugin Information

Published: 2023/07/17, Modified: 2024/10/29

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm3
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm3
- Installed package : libcups2_2.1.3-4ubuntu0.7
- Fixed package : libcups2_2.1.3-4ubuntu0.11+esm3
- Installed package : libcupscgi1_2.1.3-4ubuntu0.7
- Fixed package : libcupscgi1_2.1.3-4ubuntu0.11+esm3
- Installed package : libcupsimage2_2.1.3-4ubuntu0.7
- Fixed package : libcupsimage2_2.1.3-4ubuntu0.11+esm3
- Installed package : libcupsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcupsmime1_2.1.3-4ubuntu0.11+esm3
- Installed package : libcupspplib1_2.1.3-4ubuntu0.7
- Fixed package : libcupspplib1_2.1.3-4ubuntu0.11+esm3

[181883 - Ubuntu 16.04 ESM / 18.04 ESM : CUPS vulnerability \(USN-6361-2\)](#)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6361-2 advisory.

USN-6361-1 fixed a vulnerability in CUPS. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6361-2>

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:6361-2

Plugin Information

Published: 2023/09/26, Modified: 2024/10/29

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm5
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm5
- Installed package : libcups2_2.1.3-4ubuntu0.7
- Fixed package : libcups2_2.1.3-4ubuntu0.11+esm5
- Installed package : libcupscgi1_2.1.3-4ubuntu0.7
- Fixed package : libcupscgi1_2.1.3-4ubuntu0.11+esm5
- Installed package : libcupsimage2_2.1.3-4ubuntu0.7
- Fixed package : libcupsimage2_2.1.3-4ubuntu0.11+esm5
- Installed package : libcupsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcupsmime1_2.1.3-4ubuntu0.11+esm5

- Installed package : libcupsppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcupsppdc1_2.1.3-4ubuntu0.11+esm5

181765 - Ubuntu 16.04 ESM / 18.04 ESM : CUPS vulnerability (USN-6391-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6391-2 advisory.

USN-6391-1 fixed a vulnerability in CUPS. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6391-2>

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:6391-2

Plugin Information

Published: 2023/09/21, Modified: 2024/10/29

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm4
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm4
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm4
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm4
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm4

```
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm4

- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm4

- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm4

- Installed package : libcups2_2.1.3-4ubuntu0.7
- Fixed package : libcups2_2.1.3-4ubuntu0.11+esm4

- Installed package : libcupscgi1_2.1.3-4ubuntu0.7
- Fixed package : libcupscgi1_2.1.3-4ubuntu0.11+esm4

- Installed package : libcupsimage2_2.1.3-4ubuntu0.7
- Fixed package : libcupsimage2_2.1.3-4ubuntu0.11+esm4

- Installed package : libcupsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcupsmime1_2.1.3-4ubuntu0.11+esm4

- Installed package : libcupspdc1_2.1.3-4ubuntu0.7
- Fixed package : libcupspdc1_2.1.3-4ubuntu0.11+esm4
```

181769 - Ubuntu 16.04 ESM / 18.04 ESM : FLAC vulnerability (USN-6360-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6360-2 advisory.

USN-6360-1 fixed a vulnerability in FLAC. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6360-2>

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-2020-22219
XREF	USN:6360-2

Plugin Information

Published: 2023/09/21, Modified: 2024/10/29

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 : libflac8_1.3.1-4
- Fixed package : libflac8_1.3.1-4ubuntu0.1~esm2

182531 - Ubuntu 16.04 ESM / 18.04 ESM : GNU binutils vulnerabilities (USN-6413-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6413-1 advisory.

It was discovered that GNU binutils was not properly performing 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. This issue only affected Ubuntu 14.04 LTS. (CVE-2017-17122, CVE-2017-8421)

It was discovered that GNU binutils was not properly performing bounds checks when processing debug sections with objdump, which could lead to an overflow. 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. (CVE-2018-20671, CVE-2018-6543)

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 18.04 LTS. (CVE-2022-35205)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6413-1>

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-2017-8421
CVE	CVE-2017-17122
CVE	CVE-2018-6543
CVE	CVE-2018-20671
CVE	CVE-2022-35205
CVE	CVE-2022-47007
CVE	CVE-2022-47008
CVE	CVE-2022-47010

CVE CVE-2022-47011
CVE CVE-2022-48063
XREF USN:6413-1

Plugin Information

Published: 2023/10/04, 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.

- Installed package : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm9

184161 - Ubuntu 16.04 ESM / 18.04 ESM : Kerberos vulnerability (USN-6467-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6467-1 advisory.

Robert Morris discovered that Kerberos did not properly handle memory access when processing RPC data through kadm5, which could lead to the freeing of uninitialized memory. An authenticated remote attacker could possibly use this issue to cause kadm5 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-6467-1>

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/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:6467-1

Plugin Information

Published: 2023/11/01, Modified: 2024/09/18

Plugin Output

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 : krb5-locales_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2+esm4
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2+esm4
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2+esm4
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2+esm4
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2+esm4

178913 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6252-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6252-1 advisory.

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 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)

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 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)

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 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)

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 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 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-6252-1>

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:I:/C:A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-1184
CVE	CVE-2022-3303
CVE	CVE-2023-1611
CVE	CVE-2023-1670
CVE	CVE-2023-1859
CVE	CVE-2023-1990
CVE	CVE-2023-2124
CVE	CVE-2023-3090
CVE	CVE-2023-3111
CVE	CVE-2023-3141
CVE	CVE-2023-3268
CVE	CVE-2023-3390
CVE	CVE-2023-35001
XREF	USN:6252-1

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-214-generic for this advisory.

180532 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6342-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6342-1 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.

(CVE-2023-20593)

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 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)

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 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-6342-1>

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/Vl: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-2023-2269
CVE	CVE-2023-2985
CVE	CVE-2023-3611
CVE	CVE-2023-3776
CVE	CVE-2023-20593
CVE	CVE-2023-31084
XREF	USN:6342-1

Plugin Information

Published: 2023/09/06, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-216-generic for this advisory.

181899 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6396-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6396-1 advisory.

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)

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)

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)

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 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-6396-1>

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-2022-27672
CVE	CVE-2022-40982
CVE	CVE-2023-3212
CVE	CVE-2023-3863
CVE	CVE-2023-4128
CVE	CVE-2023-40283
XREF	USN:6396-1

Plugin Information

Published: 2023/09/26, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-218-generic for this advisory.

183457 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6440-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6440-1 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)

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)

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)

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)

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)

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)

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-6440-1>

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-2023-0597
CVE	CVE-2023-1206
CVE	CVE-2023-3772
CVE	CVE-2023-4622
CVE	CVE-2023-4623
CVE	CVE-2023-4881
CVE	CVE-2023-4921
CVE	CVE-2023-31083
CVE	CVE-2023-34319
CVE	CVE-2023-42752
CVE	CVE-2023-42753
CVE	CVE-2023-42755
XREF	USN:6440-1

Plugin Information

Published: 2023/10/20, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-219-generic for this advisory.

186083 - Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6494-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6494-1 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)

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)

It was discovered that the USB ENE card reader driver in the Linux kernel did not properly allocate enough memory when processing the storage device boot blocks. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-45862)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6494-1>

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-2023-5717
CVE	CVE-2023-31085
CVE	CVE-2023-39189
CVE	CVE-2023-39192
CVE	CVE-2023-39193
CVE	CVE-2023-39194
CVE	CVE-2023-42754
CVE	CVE-2023-45862
CVE	CVE-2023-45871
XREF	USN:6494-1

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-220-generic for this advisory.

188054 - Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerabilities (USN-6583-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6583-1 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 5.7.44 in Ubuntu 16.04 LTS and Ubuntu 18.04 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/5.7/en/news-5-7-44.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-6583-1>

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22028
CVE	CVE-2023-22084
XREF	USN:6583-1

Plugin Information

Published: 2024/01/15, 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.

- Installed package : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.44-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.44-0ubuntu0.16.04.1+esm1

183789 - Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerability (USN-6288-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6288-2 advisory.

USN-6288-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6288-2>

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-2023-22053
XREF	USN:6288-2

Plugin Information

Published: 2023/10/24, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.43-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.43-0ubuntu0.16.04.1+esm1

187955 - Ubuntu 16.04 ESM / 18.04 ESM : OpenSSH vulnerabilities (USN-6560-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6560-2 advisory.

USN-6560-1 fixed several vulnerabilities in OpenSSH. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6560-2>

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/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-48795
CVE	CVE-2023-51385
XREF	IAVA:2023-A-0703
XREF	USN:6560-2
XREF	IAVA:2023-A-0701-S

Plugin Information

Published: 2024/01/11, Modified: 2024/10/29

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 : openssh-client_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-client_1:7.2p2-4ubuntu2.10+esm5
- Installed package : openssh-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-server_1:7.2p2-4ubuntu2.10+esm5
- Installed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm5

183384 - Ubuntu 16.04 ESM / 18.04 ESM : OpenSSL vulnerabilities (USN-6435-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6435-1 advisory.

It was discovered that OpenSSL incorrectly handled excessively large Diffie-Hellman parameters. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3446)

Bernd Edlinger discovered that OpenSSL incorrectly handled excessively large Diffie-Hellman parameters. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3817)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6435-1>

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

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3446
CVE	CVE-2023-3817
XREF	IAVA:2023-A-0398-S
XREF	USN:6435-1

Plugin Information

Published: 2023/10/19, 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.

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm10

- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm10

186226 - Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerabilities (USN-6513-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6513-1 advisory.

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. (CVE-2022-48564)

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. (CVE-2023-40217)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6513-1>

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/I: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

4.8 (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-2022-48564
CVE	CVE-2023-40217
XREF	USN:6513-1

Plugin Information

Published: 2023/11/23, 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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm9
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm9
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm9
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm12
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm12
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm12
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm9
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm9
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm12
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm12

[181944 - Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerability \(USN-6400-1\)](#)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6400-1 advisory.

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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6400-1>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE-2022-48566
XREF USN:6400-1

Plugin Information

Published: 2023/09/27, 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.

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm7
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm7
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm7
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm11
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm11
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm11
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm7
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm7
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm11
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm11

177352 - Ubuntu 16.04 ESM / 18.04 ESM : Requests vulnerability (USN-6155-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6155-2 advisory.

USN-6155-1 fixed a vulnerability in Requests. This update provides the corresponding update for Ubuntu 16.04 ESM and 18.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6155-2>

Solution

Update the affected python-requests and / or python3-requests packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V/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 CVE-2023-32681
XREF USN:6155-2

Plugin Information

Published: 2023/06/15, Modified: 2024/10/29

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-requests_2.9.1-3ubuntu0.1
- Fixed package : python3-requests_2.9.1-3ubuntu0.1+esm1

184087 - Ubuntu 16.04 ESM / 18.04 ESM : X.Org X Server vulnerabilities (USN-6453-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6453-2 advisory.

USN-6453-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6453-2>

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 (CVSS:2.0/AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS:2.0/E:U/RL:OF/RC:C)

References

CVE	CVE-2023-5367
CVE	CVE-2023-5380
XREF	USN:6453-2

Plugin Information

Published: 2023/10/31, Modified: 2024/10/29

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 : `xserver-common_2:1.18.4-0ubuntu0.8`
- Fixed package : `xserver-common_2:1.18.4-0ubuntu0.12+esm6`

178443 - Ubuntu 16.04 ESM / 18.04 ESM : YAJL vulnerabilities (USN-6233-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6233-1 advisory.

It was discovered that YAJL was not properly performing bounds checks when decoding a string with escape sequences. If a user or automated system using YAJL were tricked into processing specially crafted input, an attacker could possibly use this issue to cause a denial of service (application abort). (CVE-2017-16516)

It was discovered that YAJL was not properly handling memory allocation when dealing with large inputs, which could lead to heap memory corruption. If a user or automated system using YAJL were tricked into running a specially crafted large input, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-24795)

It was discovered that memory leaks existed in one of the YAJL parsing functions. An attacker could possibly use this issue to cause a denial of service (memory exhaustion). (CVE-2023-33460)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6233-1>

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:6233-1

Plugin Information

Published: 2023/07/18, 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.

- Installed package : libyajl2_2.1.0-2
- Fixed package : libyajl2_2.1.0-2ubuntu0.16.04.1~esm1

181247 - Ubuntu 16.04 ESM / 18.04 ESM : curl vulnerabilities (USN-6237-3)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6237-3 advisory.

USN-6237-1 fixed several vulnerabilities in curl. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 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-6237-3>

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	IAVA:2023-A-0259-S
XREF	USN:6237-3

Plugin Information

Published: 2023/09/11, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm9

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm9

183750 - Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6408-2 advisory.

USN-6408-1 fixed several vulnerabilities in libXpm. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6408-2>

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: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:6408-2

Plugin Information

Published: 2023/10/23, Modified: 2024/10/29

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 : libxpm4_1:3.5.11-1ubuntu0.16.04.1
- Fixed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1+esm2

177431 - Ubuntu 16.04 ESM / 18.04 ESM : libcap2 vulnerability (USN-6166-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6166-2 advisory.

USN-6166-1 fixed a vulnerability in libcap2. This update provides the corresponding update for Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6166-2>

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/V:C: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: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-2023-2603
XREF USN:6166-2

Plugin Information

Published: 2023/06/19, Modified: 2024/10/29

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 : libcap2_1:2.24-12
- Fixed package : libcap2_1:2.24-12ubuntu0.1~esm1

- Installed package : libcap2-bin_1:2.24-12
- Fixed package : libcap2-bin_1:2.24-12ubuntu0.1~esm1

189998 - Ubuntu 16.04 ESM / 18.04 ESM : libssh vulnerabilities (USN-6592-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6592-2 advisory.

USN-6592-1 fixed vulnerabilities in libssh. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6592-2>

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:6592-2

Plugin Information

Published: 2024/02/05, Modified: 2024/10/29

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 : libssh-4_0.6.3-4.3ubuntu0.2
- Fixed package : libssh-4_0.6.3-4.3ubuntu0.6+esm1

182843 - Ubuntu 16.04 ESM / 18.04 ESM : libx11 vulnerabilities (USN-6407-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6407-2 advisory.

USN-6407-1 fixed several vulnerabilities in libx11. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6407-2>

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:6407-2

Plugin Information

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

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 : libx11-6_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-6_2:1.6.3-1ubuntu2.2+esm4
- Installed package : libx11-data_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-data_2:1.6.3-1ubuntu2.2+esm4
- Installed package : libx11-xcb1_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-xcb1_2:1.6.3-1ubuntu2.2+esm4

174752 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : OpenSSL vulnerabilities (USN-6039-1)

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-6039-1 advisory.

It was discovered that OpenSSL was not properly managing file locks when processing policy constraints. If a user or automated system were tricked into processing a certificate chain with specially crafted policy constraints, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3996)

David Benjamin discovered that OpenSSL was not properly performing the verification of X.509 certificate chains that include policy constraints, which could lead to excessive resource consumption. If a user or automated system were tricked into processing a specially crafted X.509 certificate chain that includes policy constraints, a remote attacker could possibly use this issue to cause a denial of service.

(CVE-2023-0464)

David Benjamin discovered that OpenSSL was not properly handling invalid certificate policies in leaf certificates, which would result in certain policy checks being skipped for the certificate. If a user or automated system were tricked into processing a specially crafted certificate, a remote attacker could possibly use this issue to assert invalid certificate policies and circumvent policy checking.

(CVE-2023-0465)

David Benjamin discovered that OpenSSL incorrectly documented the functionalities of function X509_VERIFY_PARAM_add0_policy, stating that it would implicitly enable certificate policy checks when doing certificate verifications, contrary to its implementation. This could cause users and applications to not perform certificate policy checks even when expected to do so. (CVE-2023-0466)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6039-1>

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

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-3996
CVE	CVE-2023-0464
CVE	CVE-2023-0466
XREF	USN:6039-1
XREF	IAVA:2022-A-0518-S
XREF	IAVA:2023-A-0158-S

Plugin Information

Published: 2023/04/25, 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.

- Installed package : libssl1.0_0.1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0_0.1.0.2g-1ubuntu4.20+esm7
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm7

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/VC:H/V:I:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-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

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 : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm3
- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm3
- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm3
- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm3
- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm3
- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm3

[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.

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

Note that Nessus has not tested 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

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 : dbus_1.10.6-1ubuntu3.3
- Fixed package : dbus_1.10.6-1ubuntu3.6+esm2
- Installed package : dbus-x11_1.10.6-1ubuntu3.3
- Fixed package : dbus-x11_1.10.6-1ubuntu3.6+esm2
- Installed package : libdbus-1-3_1.10.6-1ubuntu3.3
- Fixed package : libdbus-1-3_1.10.6-1ubuntu3.6+esm2

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-2022-38533
XREF USN:5762-1

Plugin Information

Published: 2022/12/07, 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.

- Installed package : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm5

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	CVE-2017-9937
XREF	USN:5742-1

Plugin Information

Published: 2022/11/25, 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.

- Installed package : libjbig0_2.1-3.1
- Fixed package : libjbig0_2.1-3.1ubuntu0.1~esm1

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm4

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm10

161249 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PCRE vulnerabilities (USN-5425-1)**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-5425-1 advisory.

Yunho Kim discovered that PCRE incorrectly handled memory when

handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to expose sensitive information. This issue only affects Ubuntu 18.04 LTS,

Ubuntu 20.04 LTS, Ubuntu 21.10 and Ubuntu 22.04 LTS. (CVE-2019-20838)

It was discovered that PCRE incorrectly handled memory when

handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to have unexpected behavior. This issue only affects Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-14155)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5425-1>

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-2019-20838
CVE	CVE-2020-14155
KREF	USN:5425-1

Plugin Information

Published: 2022/05/17, 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.

- Installed package : libpcre16-3_2:8.38-3.1
- Fixed package : libpcre16-3_2:8.38-3.1ubuntu0.1~esm1

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-2020-16156
XREF USN:5689-1

Plugin Information

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

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 : libperl15.22_5.22.1-9ubuntu0.6
- Fixed package : libperl15.22_5.22.1-9ubuntu0.9+esm1
- Installed package : perl_5.22.1-9ubuntu0.6
- Fixed package : perl_5.22.1-9ubuntu0.9+esm1
- Installed package : perl-base_5.22.1-9ubuntu0.6
- Fixed package : perl-base_5.22.1-9ubuntu0.9+esm1
- Installed package : perl-modules-5.22_5.22.1-9ubuntu0.6
- Fixed package : perl-modules-5.22_5.22.1-9ubuntu0.9+esm1

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

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_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm1

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 handled 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

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 : libaprutil1_1.5.4-1build1
- Fixed package : libaprutil1_1.5.4-1ubuntu0.1~esm2
- Installed package : libaprutil1-dbd-sqlite3_1.5.4-1build1
- Fixed package : libaprutil1-dbd-sqlite3_1.5.4-1ubuntu0.1~esm2
- Installed package : libaprutil1-ldap_1.5.4-1build1
- Fixed package : libaprutil1-ldap_1.5.4-1ubuntu0.1~esm2

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

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 : e2fslibs_1.42.13-1ubuntu1
- Fixed package : e2fslibs_1.42.13-1ubuntu1.2+esm1
- Installed package : e2fsprogs_1.42.13-1ubuntu1
- Fixed package : e2fsprogs_1.42.13-1ubuntu1.2+esm1
- Installed package : libcomerr2_1.42.13-1ubuntu1
- Fixed package : libcomerr2_1.42.13-1ubuntu1.2+esm1
- Installed package : libss2_1.42.13-1ubuntu1
- Fixed package : libss2_1.42.13-1ubuntu1.2+esm1

161219 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : libxml2 vulnerabilities (USN-5422-1)

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-5422-1 advisory.

Shinji Sato discovered that libxml2 incorrectly handled certain XML files. 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 14.04 ESM, and Ubuntu 16.04 ESM. (CVE-2022-23308)

It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-29824)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5422-1>

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 (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-2022-23308
CVE	CVE-2022-29824
XREF	USN:5422-1

Plugin Information

Published: 2022/05/16, 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.

- Installed package : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm2

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE [CVE-2022-3328](#)
XREF USN:5753-1

Plugin Information

Published: 2022/12/01, Modified: 2024/08/29

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 : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.54.3+16.04.0ubuntu0.1~esm5

- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.54.3+16.04.0ubuntu0.1~esm5

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

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 : `libpam-systemd_229-4ubuntu21.16`
- Fixed package : `libpam-systemd_229-4ubuntu21.31+esm3`

- Installed package : libsystemd0_229-4ubuntu21.16
- Fixed package : libsystemd0_229-4ubuntu21.31+esm3
- Installed package : libudev1_229-4ubuntu21.16
- Fixed package : libudev1_229-4ubuntu21.31+esm3
- Installed package : systemd_229-4ubuntu21.16
- Fixed package : systemd_229-4ubuntu21.31+esm3
- Installed package : systemd-sysv_229-4ubuntu21.16
- Fixed package : systemd-sysv_229-4ubuntu21.31+esm3
- Installed package : udev_229-4ubuntu21.16
- Fixed package : udev_229-4ubuntu21.31+esm3

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	CVE-2022-48303
XREF	USN:5900-1

Plugin Information

Published: 2023/03/01, 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.

- Installed package : tar_1.28-2.1ubuntu0.1
- Fixed package : tar_1.28-2.1ubuntu0.2+esm2

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

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 : unzip_6.0-20ubuntu1
- Fixed package : unzip_6.0-20ubuntu1.1+esm1

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

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 : aspell_0.60.7~20110707-3build1
- Fixed package : aspell_0.60.7~20110707-3ubuntu0.1+esm1
- Installed package : libaspell15_0.60.7~20110707-3build1
- Fixed package : libaspell15_0.60.7~20110707-3ubuntu0.1+esm1

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

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 : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3+esm2
- Installed package : bluez-cups_5.37-0ubuntu5.1
- Fixed package : bluez-cups_5.37-0ubuntu5.3+esm2
- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3+esm2
- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3+esm2

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

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 : libexiv2-14_0.25-2.1ubuntu16.04.3
- Fixed package : libexiv2-14_0.25-2.1ubuntu16.04.7+esm1

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

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 : libexiv2-14_0.25-2.1ubuntu16.04.3
- Fixed package : libexiv2-14_0.25-2.1ubuntu16.04.7+esm2

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

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 : libexiv2-14_0.25-2.1ubuntu16.04.3
- Fixed package : libexiv2-14_0.25-2.1ubuntu16.04.7+esm4

153137 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GD library vulnerabilities (USN-5068-1)

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-5068-1 advisory.

It was discovered that GD Graphics Library incorrectly handled certain GD

and GD2 files. An attacker could possibly use this issue to cause a crash or expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, Ubuntu 16.04 ESM, and Ubuntu 14.04 ESM. (CVE-2017-6363)

It was discovered that GD Graphics Library incorrectly handled certain TGA files. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2021-381)

It was discovered that GD Graphics Library incorrectly handled certain files. An attacker could possibly use this issue to cause a crash. (CVE-2021-40145)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5068-1>

Solution

Update the affected libgd-dev, libgd-tools and / or libgd3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-6363
CVE	CVE-2021-38115
CVE	CVE-2021-40145
XREF	USN:5068-1

Plugin Information

Published: 2021/09/08, 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.

- Installed package : libgd3_2.1.1-4ubuntu0.16.04.10
- Fixed package : libgd3_2.1.1-4ubuntu0.16.04.12+esm1

166088 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GMP vulnerability (USN-5672-1)

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-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 (CVSS:2.0/AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS:2.0/E:POC/RL:OF/RC:C)

References

CVE-2021-43618
XREF-USN:5672-1

Plugin Information

Published: 2022/10/13, 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.

- Installed package : libgmp10_2:6.1.0+dfsg-2
- Fixed package : libgmp10_2:6.1.0+dfsg-2ubuntu0.1~esm1

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	CVE-2021-39365
XREF	USN:5055-1

Plugin Information

Published: 2021/08/31, 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.

- Installed package : libgrilo-0.2-1_0.2.15-1
- Fixed package : libgrilo-0.2-1_0.2.15-1ubuntu0.1~esm1

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

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-gst-plugins-base-1.0_1.8.3-1ubuntu0.2
- Fixed package : gir1.2-gst-plugins-base-1.0_1.8.3-1ubuntu0.3+esm1
- Installed package : gstreamer1.0-alsa_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-alsa_1.8.3-1ubuntu0.3+esm1
- Installed package : gstreamer1.0-plugins-base_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-plugins-base_1.8.3-1ubuntu0.3+esm1
- Installed package : gstreamer1.0-plugins-base-apps_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-plugins-base-apps_1.8.3-1ubuntu0.3+esm1
- Installed package : gstreamer1.0-x_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-x_1.8.3-1ubuntu0.3+esm1
- Installed package : libgstreamer-plugins-base1.0-0_1.8.3-1ubuntu0.2
- Fixed package : libgstreamer-plugins-base1.0-0_1.8.3-1ubuntu0.3+esm1

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

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 : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20210608.0ubuntu0.16.04.1+esm1

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

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 : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm1

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-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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-210-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 Schrurer 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

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm1
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm1
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm1
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm2
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm2
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm2
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm1
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm1
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm2
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm2

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	CVE-2020-23903
XREF	USN:5280-1

Plugin Information

Published: 2022/02/10, 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.

- Installed package : `libspeex1_1.2~rc1.2-1ubuntu1`
- Fixed package : `libspeex1_1.2~rc1.2-1ubuntu1+esm1`
- Installed package : `libspeexdsp1_1.2~rc1.2-1ubuntu1`
- Fixed package : `libspeexdsp1_1.2~rc1.2-1ubuntu1+esm1`

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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm2
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm2
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm2
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm2

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 possible 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 possible 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 possible 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 possible 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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm3
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm3
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm3
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm3

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

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 : libcaca0_0.99.beta19-2ubuntu0.16.04.1
- Fixed package : libcaca0_0.99.beta19-2ubuntu0.16.04.2+esm1

163871 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libxml2 vulnerability (USN-5548-1)

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-5548-1 advisory.

It was discovered that libxml2 incorrectly handled certain XML 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-5548-1>

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

5.5 (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-2016-3709
XREF	USN:5548-1

Plugin Information

Published: 2022/08/05, 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.

- Installed package : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7+esm3

156650 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : lxml vulnerability (USN-5225-1)

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-5225-1 advisory.

It was discovered that lxml incorrectly handled certain XML and HTML 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-5225-1>

Solution

Update the affected python-lxml and / or python3-lxml packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.2 (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
XREF

[CVE-2021-43818](#)
USN:5225-1

Plugin Information

Published: 2022/01/12, 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.

- Installed package : python3-lxml_3.5.0-1ubuntu0.1
- Fixed package : python3-lxml_3.5.0-1ubuntu0.4+esm2

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/VI:H/V/A: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

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 : tar_1.28-2.1ubuntu0.1
- Fixed package : tar_1.28-2.1ubuntu0.2+esm1

160980 - Ubuntu 16.04 ESM / 18.04 LTS : Cron regression (USN-5259-3)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5259-3 advisory.

USN-5259-1 and USN-5259-2 fixed vulnerabilities in Cron. 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-5259-3>

Solution

Update the affected cron 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-9525
XREF	USN:5259-3

Plugin Information

Published: 2022/05/11, Modified: 2024/10/29

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 : cron_3.0pl1-128ubuntu2
- Fixed package : cron_3.0pl1-128ubuntu2+esm2

169510 - Ubuntu 16.04 ESM / 18.04 LTS : DjVuLibre vulnerability (USN-5005-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5005-1 advisory.

It was discovered that DjVuLibre incorrectly handled certain djvu 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-5005-1>

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-2021-3630
XREF	USN:5005-1

Plugin Information

Published: 2023/01/04, 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.

- Installed package : libdjvulibre-text_3.5.27.1-5
- Fixed package : libdjvulibre-text_3.5.27.1-5ubuntu0.1+esm2

- Installed package : libdjvulibre21_3.5.27.1-5
- Fixed package : libdjvulibre21_3.5.27.1-5ubuntu0.1+esm2

156040 - Ubuntu 16.04 ESM / 18.04 LTS : GLib vulnerability (USN-5189-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5189-1 advisory.

It was discovered that GLib incorrectly handled certain environment variables. 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-5189-1>

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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3800
XREF	USN:5189-1

Plugin Information

Published: 2021/12/13, 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.

- Installed package : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.8+esm1

- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.8+esm1

- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.8+esm1

154903 - Ubuntu 16.04 ESM / 18.04 LTS : ICU vulnerability (USN-5133-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5133-1 advisory.

It was discovered that ICU contains a use after free issue. An attacker could use this issue to cause a denial of service with crafted input.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5133-1>

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-2020-21913](#)
XREF USN:5133-1

Plugin Information

Published: 2021/11/05, 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.

- Installed package : libicu55_55.1-7ubuntu0.4
- Fixed package : libicu55_55.1-7ubuntu0.5+esm1

155729 - Ubuntu 16.04 ESM / 18.04 LTS : ImageMagick vulnerabilities (USN-5158-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5158-1 advisory.

It was discovered that ImageMagick incorrectly handled certain values when processing visual effects based image files. By tricking a user into opening a specially

crafted image file, an attacker could crash the application causing a denial of service. (CVE-2021-20244)

It was discovered that ImageMagick incorrectly handled certain values when performing resampling operations. By tricking a user into opening a specially crafted image file, an attacker could crash the application

causing a denial of service. (CVE-2021-20246)

It was discovered that ImageMagick incorrectly handled certain values when processing visual effects based image files. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service (CVE-2021-20309)

It was discovered that ImageMagick incorrectly handled certain values when processing thumbnail image data. By tricking a user into opening a specially crafted image file, an attacker could crash the application

causing a denial of service. (CVE-2021-20312)

It was discovered that ImageMagick incorrectly handled memory cleanup when performing certain cryptographic operations. Under certain conditions sensitive cryptographic information could be disclosed.

(CVE-2021-20313)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5158-1>

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

6.5 (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-2021-20244
CVE	CVE-2021-20246
CVE	CVE-2021-20309
CVE	CVE-2021-20312
CVE	CVE-2021-20313
XREF	USN:5158-1
XREF	IAVB:2021-B-0017-S

Plugin Information

Published: 2021/11/30, 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.

- Installed package : `imagemagick_8:6.8.9.9-7ubuntu5.13`
- Fixed package : `imagemagick_8:6.8.9.9-7ubuntu5.16+esm1`

- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm1
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm1
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm1
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm1
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm1

168160 - Ubuntu 16.04 ESM / 18.04 LTS : ImageMagick vulnerabilities (USN-5736-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5736-1 advisory.

It was discovered that ImageMagick incorrectly handled certain values when processing PDF files. If a user or automated system using ImageMagick were tricked into opening a specially crafted PDF file, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2021-20224)

Zhang Xiaohui discovered that ImageMagick incorrectly handled certain values when processing image data.

If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 22.10. (CVE-2021-20241)

Zhang Xiaohui discovered that ImageMagick incorrectly handled certain values when processing image data.

If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 22.10. (CVE-2021-20243)

It was discovered that ImageMagick incorrectly handled certain values when processing visual effects based image files. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-20244)

It was discovered that ImageMagick could be made to divide by zero when processing crafted files. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-20245)

It was discovered that ImageMagick incorrectly handled certain values when performing resampling operations. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-20246)

It was discovered that ImageMagick incorrectly handled certain values when processing visual effects based image files. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-20309)

It was discovered that ImageMagick incorrectly handled certain values when processing thumbnail image data. By tricking a user into opening a specially crafted image file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-20312)

It was discovered that ImageMagick incorrectly handled memory cleanup when performing certain cryptographic operations. Under certain conditions sensitive cryptographic information could be disclosed.

This issue only affected Ubuntu 22.10. (CVE-2021-20313)

It was discovered that ImageMagick did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted file using the convert command, an attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-3574)

It was discovered that ImageMagick did not use the correct rights when specifically excluded by a module policy. An attacker could use this issue to read and write certain restricted files. This issue only affected Ubuntu 22.10. (CVE-2021-39212)

It was discovered that ImageMagick incorrectly handled certain values when processing specially crafted SVG files. By tricking a user into opening a specially crafted SVG file, an attacker could crash the application causing a denial of service. This issue only affected Ubuntu 22.10. (CVE-2021-4219)

It was discovered that ImageMagick did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted DICOM file, an attacker could possibly use this issue to cause ImageMagick to crash, resulting in a denial of service, or expose sensitive information. This issue only affected Ubuntu 22.10. (CVE-2022-1114)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 22.10. (CVE-2022-28463)

It was discovered that ImageMagick incorrectly handled certain values. If a user were tricked into processing a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 22.10.

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into processing a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 22.10. (CVE-2022-32547)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5736-1>

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-2021-3574
CVE	CVE-2021-4219
CVE	CVE-2021-20224
CVE	CVE-2021-20241
CVE	CVE-2021-20243
CVE	CVE-2021-20244
CVE	CVE-2021-20245
CVE	CVE-2021-20246
CVE	CVE-2021-20309
CVE	CVE-2021-20312
CVE	CVE-2021-20313
CVE	CVE-2021-39212
CVE	CVE-2022-1114
CVE	CVE-2022-28463
CVE	CVE-2022-32545
CVE	CVE-2022-32546
CVE	CVE-2022-32547
XREF	USN:5736-1

Plugin Information

Published: 2022/11/24, 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.

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm5
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm5
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm5
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm5

- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm5
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm5

161759 - Ubuntu 16.04 ESM / 18.04 LTS : ImageMagick vulnerability (USN-5456-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5456-1 advisory.

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5456-1>

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-2022-28463
XREF	USN:5456-1

Plugin Information

Published: 2022/06/01, 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.

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm3
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm3
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm3
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm3
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm3

- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm3

150952 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5003-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5003-1 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)

It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. (CVE-2021-3600)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5003-1>

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3600
CVE	CVE-2021-3609
CVE	CVE-2021-23133
XREF	USN:5003-1

Plugin Information

Published: 2021/06/23, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-147-generic for this advisory.

152640 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5044-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5044-1 advisory.

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-5044-1>

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
XREF	USN:5044-1

Plugin Information

Published: 2021/08/18, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-154-generic for this advisory.

154273 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5114-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5114-1 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)

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 ext4 file system in the Linux kernel contained a race condition when writing xattrs 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-5114-1>

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-3702
CVE	CVE-2021-38198
CVE	CVE-2021-40490
CVE	CVE-2021-42008
XREF	USN:5114-1

Plugin Information

Published: 2021/10/20, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-161-generic for this advisory.

154972 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5136-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5136-1 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 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-2020-36322)

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)

Ilya 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 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)

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 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-5136-1>

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-2020-36322
CVE	CVE-2020-36385
CVE	CVE-2021-3655
CVE	CVE-2021-3743
CVE	CVE-2021-3753
CVE	CVE-2021-3759
CVE	CVE-2021-38199
CVE	CVE-2021-42252
XREF	USN:5136-1

Plugin Information

Published: 2021/11/09, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-162-generic for this advisory.

155747 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5164-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5164-1 advisory.

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-5164-1>

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-2021-3744
CVE	CVE-2021-3764
CVE	CVE-2021-37159
XREF	USN:5164-1

Plugin Information

Published: 2021/12/01, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-163-generic for this advisory.

160065 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5385-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5385-1 advisory.

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)

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-5385-1>

Solution

Update the affected kernel 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/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-2021-43975
CVE	CVE-2022-0617
CVE	CVE-2022-24448
CVE	CVE-2022-24959
XREF	USN:5385-1

Plugin Information

Published: 2022/04/21, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-176-generic for this advisory.

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5418-1 advisory.

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)

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-2022-23042)

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 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 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)

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-5418-1>

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

7.7 (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-2021-26401
CVE	CVE-2022-23036
CVE	CVE-2022-23037
CVE	CVE-2022-23038
CVE	CVE-2022-23039
CVE	CVE-2022-23040
CVE	CVE-2022-23042
CVE	CVE-2022-24958
CVE	CVE-2022-25258
CVE	CVE-2022-25375

CVE	CVE-2022-26490
CVE	CVE-2022-26966
CVE	CVE-2022-27223
XREF	USN:5418-1

Plugin Information

Published: 2022/05/12, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-177-generic for this advisory.

161954 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5466-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5466-1 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)

It was discovered that the btrfs file system implementation in the Linux kernel did not properly handle locking in certain error conditions. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2021-4149)

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 virtual graphics memory manager implementation in the Linux kernel was subject to a race condition, potentially leading to an information leak. (CVE-2022-1419)

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 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-5466-1>

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

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-2021-3772
CVE	CVE-2021-4149
CVE	CVE-2022-1016
CVE	CVE-2022-1419
CVE	CVE-2022-21499
CVE	CVE-2022-28356
CVE	CVE-2022-28390
XREF	USN:5466-1

Plugin Information

Published: 2022/06/08, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-184-generic for this advisory.

165286 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5621-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5621-1 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)

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-5621-1>

Solution

Update the affected kernel 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

5.8 (CVSS:3.0/E:U/RL: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

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

References

CVE	CVE-2021-33655
CVE	CVE-2022-36946
XREF	USN:5621-1

Plugin Information

Published: 2022/09/21, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-193-generic for this advisory.

167770 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5727-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5727-1 advisory.

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)

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 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)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5727-1>

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-2022-2153
CVE	CVE-2022-2978
CVE	CVE-2022-3028
CVE	CVE-2022-3635
CVE	CVE-2022-20422
CVE	CVE-2022-36879
CVE	CVE-2022-40768
XREF	USN:5727-1

Plugin Information

Published: 2022/11/17, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-197-generic for this advisory.

169692 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5790-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5790-1 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 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)

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)

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)

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)

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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5790-1>

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-2021-4159
CVE	CVE-2022-3061
CVE	CVE-2022-3586
CVE	CVE-2022-4095
CVE	CVE-2022-20421
CVE	CVE-2022-39188
CVE	CVE-2022-40307
XREF	USN:5790-1

Plugin Information

Published: 2023/01/07, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-201-generic for this advisory.

174459 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6029-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6029-1 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)

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)

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-6029-1>

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-2022-3903
CVE	CVE-2023-1073
CVE	CVE-2023-1074
CVE	CVE-2023-1281
CVE	CVE-2023-26545
XREF	USN:6029-1

Plugin Information

Published: 2023/04/19, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-209-generic for this advisory.

176227 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6095-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6095-1 advisory.

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)

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-6095-1>

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:O/RC:C)

References

CVE	CVE-2023-0459
CVE	CVE-2023-1118
CVE	CVE-2023-1513
CVE	CVE-2023-2162
CVE	CVE-2023-32269
XREF	USN:6095-1

Plugin Information

Published: 2023/05/23, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-211-generic for this advisory.

176565 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6130-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6130-1 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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-6130-1>

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-2023-30456
CVE	CVE-2023-31436
CVE	CVE-2023-32233
XREF	USN:6130-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2023/06/01, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-212-generic for this advisory.

159372 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerability (USN-5357-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5357-1 advisory.

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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5357-1>

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-2022-27666
XREF USN:5357-1

Exploitable With

CANVAS (true)

Plugin Information

Published: 2022/03/31, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-175-generic for this advisory.

155296 - Ubuntu 16.04 ESM / 18.04 LTS : OpenEXR vulnerability (USN-5144-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5144-1 advisory.

It was discovered that OpenEXR incorrectly handled certain EXR image 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-5144-1>

Solution

Update the affected libopenexr-dev, libopenexr22 and / or openexr 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-2021-3933](#)
XREF USN:5144-1

Plugin Information

Published: 2021/11/12, 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.

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.6+esm2

170960 - Ubuntu 16.04 ESM : Apache HTTP Server vulnerability (USN-5839-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5839-2 advisory.

USN-5839-1 fixed a vulnerability in Apache. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5839-2>

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-37436
XREF	USN:5839-2
XREF	IAVA:2023-A-0047-S

Plugin Information

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

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm9
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm9
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm9
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm9

153366 - Ubuntu 16.04 ESM : Apport vulnerabilities (USN-5077-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5077-2 advisory.

USN-5077-1 fixed several vulnerabilities in Apport. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5077-2>

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:5077-2

Plugin Information

Published: 2021/09/14, Modified: 2024/10/29

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 : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30+esm2
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30+esm2
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30+esm2
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30+esm2

168280 - Ubuntu 16.04 ESM : Bind vulnerabilities (USN-5747-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5747-1 advisory.

It was discovered that Bind incorrectly handled large query name when using lightweight resolver protocol. A remote attacker could use this issue to consume resources, leading to a denial of service.
(CVE-2016-2775)

It was discovered that Bind incorrectly handled large zone data size received via AXFR response. A remote authenticated attacker could use this issue to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS. (CVE-2016-6170)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5747-1>

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

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

|

References

CVE	CVE-2016-2775
CVE	CVE-2016-6170
XREF	USN:5747-1
XREF	IAVA:2017-A-0004
XREF	IAVA:2016-A-0194-S

Plugin Information

Published: 2022/11/29, 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.

- Installed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm5

154709 - Ubuntu 16.04 ESM : Bind vulnerability (USN-5126-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5126-2 advisory.

USN-5126-1 fixed a vulnerability in Bind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5126-2>

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

I

References

CVE	CVE-2021-25219
XREF	USN:5126-2
XREF	IAVA:2021-A-0525-S

Plugin Information

Published: 2021/10/29, Modified: 2024/10/29

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 : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm1

[159020 - Ubuntu 16.04 ESM : Bind vulnerability \(USN-5332-2\)](#)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5332-2 advisory.

USN-5332-1 fixed a vulnerability in Bind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5332-2>

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 (CVSS:2.0/AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS:2.0/E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-25220
XREF	USN:5332-2
XREF	IAVA:2022-A-0122-S

Plugin Information

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

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 : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19+esm2

160896 - Ubuntu 16.04 ESM : BusyBox vulnerability (USN-5179-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5179-2 advisory.

USN-5179-1 fixed vulnerabilities in BusyBox. This update provides the corresponding updates for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5179-2>

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/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

6.5 (CVSS:3.0/E:U/R:L/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-2021-28831
XREF	USN:5179-2

Plugin Information

Published: 2022/05/10, Modified: 2024/10/29

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 : busybox-initramfs_1:1.22.0-15ubuntu1
- Fixed package : busybox-initramfs_1:1.22.0-15ubuntu1.4+esm1
- Installed package : busybox-static_1:1.22.0-15ubuntu1
- Fixed package : busybox-static_1:1.22.0-15ubuntu1.4+esm1

176561 - Ubuntu 16.04 ESM : CUPS vulnerability (USN-6128-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6128-2 advisory.

USN-6128-1 fixed a vulnerability in CUPS. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-6128-2>

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

4.9 (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:6128-2

Plugin Information

Published: 2023/06/01, Modified: 2024/10/29

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm2
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm2
- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.11+esm2
- Installed package : libcurlcgi1_2.1.3-4ubuntu0.7
- Fixed package : libcurlcgi1_2.1.3-4ubuntu0.11+esm2

```
- Installed package : libcupsimage2_2.1.3-4ubuntu0.7
- Fixed package : libcupsimage2_2.1.3-4ubuntu0.11+esm2

- Installed package : libcupsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcupsmime1_2.1.3-4ubuntu0.11+esm2

- Installed package : libcupspdc1_2.1.3-4ubuntu0.7
- Fixed package : libcupspdc1_2.1.3-4ubuntu0.11+esm2
```

160959 - Ubuntu 16.04 ESM : Cairo vulnerabilities (USN-5407-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5407-1 advisory.

Gustavo Grieco, Alberto Garcia, Francisco Oca, Suleman Ali, and others discovered that Cairo incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service.

(CVE-2016-9082, CVE-2017-9814, CVE-2019-6462)

Stephan Bergmann discovered that Cairo incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-35492)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5407-1>

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-2016-9082
CVE	CVE-2017-9814
CVE	CVE-2019-6462
CVE	CVE-2020-35492
XREF	USN:5407-1

Plugin Information

Published: 2022/05/10, 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.

- Installed package : libcairo-gobject2_1.14.6-1

- Fixed package : libcairo-gobject2_1.14.6-1ubuntu0.1~esm1
- Installed package : libcairo2_1.14.6-1
- Fixed package : libcairo2_1.14.6-1ubuntu0.1~esm1

157299 - Ubuntu 16.04 ESM : Cron vulnerabilities (USN-5259-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5259-1 advisory.

It was discovered that the postinst maintainer script in Cron unsafely handled file permissions during package install or update operations. An attacker could possibly use this issue to perform a privilege escalation attack. (CVE-2017-9525)

Florian Weimer discovered that Cron incorrectly handled certain memory operations during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9704)

It was discovered that Cron incorrectly handled user input during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9705)

It was discovered that Cron contained a use-after-free vulnerability in its force_rescan_user function. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9706)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5259-1>

Solution

Update the affected cron 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/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-2017-9525
CVE	CVE-2019-9704
CVE	CVE-2019-9705
CVE	CVE-2019-9706
XREF	USN:5259-1

Plugin Information

Published: 2022/02/01, 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.

- Installed package : cron_3.0p11-128ubuntu2
- Fixed package : cron_3.0p11-128ubuntu2+esm1

158271 - Ubuntu 16.04 ESM : Cyrus SASL vulnerability (USN-5301-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5301-2 advisory.

USN-5301-1 fixed a vulnerability in Cyrus. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5301-2>

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:5301-2

Plugin Information

Published: 2022/02/23, Modified: 2024/08/29

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 : libsasl2-2_2.1.26.dfsg1-14ubuntu0.1
- Fixed package : libsasl2-2_2.1.26.dfsg1-14ubuntu0.2+esm1
- Installed package : libsasl2-modules_2.1.26.dfsg1-14ubuntu0.1
- Fixed package : libsasl2-modules_2.1.26.dfsg1-14ubuntu0.2+esm1
- Installed package : libsasl2-modules-db_2.1.26.dfsg1-14ubuntu0.1
- Fixed package : libsasl2-modules-db_2.1.26.dfsg1-14ubuntu0.2+esm1

181452 - Ubuntu 16.04 ESM : DBus vulnerability (USN-6372-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6372-1 advisory.

It was discovered that DBus incorrectly handled certain invalid messages. A local attacker could possibly use this issue to cause DBus 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-6372-1>

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-2023-34969](#)
XREF USN:6372-1

Plugin Information

Published: 2023/09/14, 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.

- Installed package : dbus_1.10.6-1ubuntu3.3
- Fixed package : dbus_1.10.6-1ubuntu3.6+esm3
- Installed package : dbus-x11_1.10.6-1ubuntu3.3
- Fixed package : dbus-x11_1.10.6-1ubuntu3.6+esm3
- Installed package : libdbus-1-3_1.10.6-1ubuntu3.3
- Fixed package : libdbus-1-3_1.10.6-1ubuntu3.6+esm3

167065 - Ubuntu 16.04 ESM : DHCP vulnerabilities (USN-5658-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5658-2 advisory.

USN-5658-1 fixed vulnerabilities in DHCP. This update provides the corresponding updates for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5658-2>

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)

References

CVE	CVE-2022-2928
CVE	CVE-2022-2929
XREF	USN:5658-2

Plugin Information

Published: 2022/11/08, Modified: 2024/10/29

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 : isc-dhcp-client_4.3.3-5ubuntu12.10
- Fixed package : isc-dhcp-client_4.3.3-5ubuntu12.10+esm2
- Installed package : isc-dhcp-common_4.3.3-5ubuntu12.10
- Fixed package : isc-dhcp-common_4.3.3-5ubuntu12.10+esm2

149651 - Ubuntu 16.04 ESM : DjVuLibre vulnerabilities (USN-4957-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4957-2 advisory.

USN-4957-1 fixed several vulnerabilities in DjVuLibre. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4957-2>

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

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:4957-2

Plugin Information

Published: 2021/05/18, Modified: 2024/10/29

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 : libdjavulibre-text_3.5.27.1-5
- Fixed package : libdjavulibre-text_3.5.27.1-5ubuntu0.1+esm1
- Installed package : libdjavulibre21_3.5.27.1-5
- Fixed package : libdjavulibre21_3.5.27.1-5ubuntu0.1+esm1

164828 - Ubuntu 16.04 ESM : Dnsmasq vulnerability (USN-4976-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-4976-2 advisory.

USN-4976-1 fixed a vulnerability in Dnsmasq. This update provides the corresponding update for Ubuntu 16.04 ESM.

Dnsmasq has been updated to 2.79-1 for Ubuntu 16.04 ESM in order to fix some security issues.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4976-2>

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
XREF

CVE-2021-3448
USN:4976-2

Plugin Information

Published: 2022/09/07, Modified: 2024/10/29

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 : dnsmasq-base_2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.79-1ubuntu0.16.04.1+esm1

158939 - Ubuntu 16.04 ESM : FUSE vulnerability (USN-5326-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5326-1 advisory.

It was discovered that FUSE is susceptible to a restriction bypass flaw on a system that has SELinux active. A local attacker with non-root privileges could mount a FUSE file system that is accessible to other users and trick them into accessing files on that file system, which

could result in a Denial of Service or other unspecified conditions.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5326-1>

Solution

Update the affected fuse, libfuse-dev and / or libfuse2 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-2018-10906
XREF	USN:5326-1

Plugin Information

Published: 2022/03/15, Modified: 2024/08/29

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 : fuse_2.9.4-1ubuntu3.1
- Fixed package : fuse_2.9.4-1ubuntu3.1+esm1
- Installed package : libfuse2_2.9.4-1ubuntu3.1
- Fixed package : libfuse2_2.9.4-1ubuntu3.1+esm1

161671 - Ubuntu 16.04 ESM : FreeType vulnerability (USN-5453-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5453-1 advisory.

It was discovered that FreeType incorrectly handled certain font 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-5453-1>

Solution

Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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
XREF
CVE-2022-27406
USN:5453-1

Plugin Information

Published: 2022/05/30, 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.

- Installed package : libfreetype6_2.6.1-0.1ubuntu2.3
- Fixed package : libfreetype6_2.6.1-0.1ubuntu2.5+esm1

166514 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5699-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5699-1 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. (CVE-2021-3326)

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. (CVE-2021-35942)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5699-1>

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:O/RC:C)

References

CVE	CVE-2021-3326
CVE	CVE-2021-35942
XREF	USN:5699-1

Plugin Information

Published: 2022/10/26, 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.

- Installed package : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm2
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm2
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm2
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm2
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm2
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm2

168533 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5768-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5768-1 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.

(CVE-2016-10228, CVE-2019-25013, CVE-2020-27618)

It was discovered that the GNU C Library did not properly handle DNS responses when ENDSO is enabled. An attacker could possibly use this issue to cause fragmentation-based attacks. (CVE-2017-12132)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5768-1>

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

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-2016-10228
CVE	CVE-2017-12132
CVE	CVE-2019-25013
CVE	CVE-2020-27618
XREF	USN:5768-1

Plugin Information

Published: 2022/12/08, Modified: 2025/02/20

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm3
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm3
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm3
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm3
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm3
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm3

159138 - Ubuntu 16.04 ESM : GNU binutils vulnerabilities (USN-5341-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5341-1 advisory.

It was discovered that GNU binutils incorrectly handled checks for memory allocation when parsing relocs in a corrupt file. An attacker could possibly use this issue to cause a denial of service.
(CVE-2017-17122)

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)

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. (CVE-2021-45078)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5341-1>

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-2017-17122
CVE	CVE-2021-3487
CVE	CVE-2021-45078
XREF	USN:5341-1

Plugin Information

Published: 2022/03/22, Modified: 2024/08/29

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 : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm3

159248 - Ubuntu 16.04 ESM : GNU binutils vulnerability (USN-5349-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5349-1 advisory.

It was discovered that GNU binutils gold incorrectly handled certain 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-5349-1>

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-2019-1010204
XREF	USN:5349-1

Plugin Information

Published: 2022/03/28, 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.

- Installed package : binutils_2.26.1-1ubuntu1~16.04.8
- Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm4

157224 - Ubuntu 16.04 ESM : GNU cpio vulnerability (USN-5064-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5064-2 advisory.

USN-5064-1 fixed vulnerabilities in GNU cpio. This update provides the corresponding updates for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5064-2>

Solution

Update the affected cpio 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

7.0 (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:5064-2

Plugin Information

Published: 2022/01/28, Modified: 2024/10/29

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 : cpio_2.11+dfsg-5ubuntu1
- Fixed package : cpio_2.11+dfsg-5ubuntu1.1+esm1

179902 - Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6291-1 advisory.

Hanno Bock discovered that GStreamer incorrectly handled certain datetime strings. An attacker could possibly use this issue to cause a denial of service 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-6291-1>

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-2017-5838
XREF	USN:6291-1

Plugin Information

Published: 2023/08/16, 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.

- Installed package : gir1.2-gstreamer-1.0_1.8.3-1~ubuntu0.1
- Fixed package : gir1.2-gstreamer-1.0_1.8.3-1~ubuntu0.1+esm1
- Installed package : gstreamer1.0-tools_1.8.3-1~ubuntu0.1
- Fixed package : gstreamer1.0-tools_1.8.3-1~ubuntu0.1+esm1
- Installed package : libgstreamer1.0-0_1.8.3-1~ubuntu0.1
- Fixed package : libgstreamer1.0-0_1.8.3-1~ubuntu0.1+esm1

156743 - Ubuntu 16.04 ESM : Ghostscript vulnerabilities (USN-5224-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5224-2 advisory.

USN-5224-1 fixed several vulnerabilities in Ghostscript. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5224-2>

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-2021-45944
CVE	CVE-2021-45949
XREF	USN:5224-2

Plugin Information

Published: 2022/01/13, Modified: 2024/08/29

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 : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm1`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm1`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm1`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm1`

161983 - Ubuntu 16.04 ESM : Ghostscript vulnerability (USN-5396-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5396-2 advisory.

USN-5396-1 addressed a vulnerability in Ghostscript. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5396-2>

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

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-2019-25059](#)
XREF USN:5396-2

Plugin Information

Published: 2022/06/09, Modified: 2024/10/29

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 : `ghostscript_9.26~dfsg+0-0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0-0ubuntu0.16.04.14+esm3`
- Installed package : `ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.14+esm3`
- Installed package : `libgs9_9.26~dfsg+0-0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0-0ubuntu0.16.04.14+esm3`
- Installed package : `libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.14+esm3`

165278 - Ubuntu 16.04 ESM : Ghostscript vulnerability (USN-5618-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5618-1 advisory.

It was discovered the Ghostscript incorrectly handled memory when processing certain inputs. By tricking a user into opening a specially crafted PDF file, an attacker could cause the program to 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-5618-1>

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-27792
XREF	USN:5618-1
XREF	IAVB:2022-B-0034-S

Plugin Information

Published: 2022/09/21, 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.

- Installed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm4`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm4`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm4`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm4`

163026 - Ubuntu 16.04 ESM : GnuPG vulnerability (USN-5503-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5503-2 advisory.

USN-5503-1 fixed a vulnerability in GnuPG. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5503-2>

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:5503-2

Plugin Information

Published: 2022/07/12, Modified: 2024/10/29

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 : dirmngr_2.1.11-6ubuntu2.1
- Fixed package : dirmngr_2.1.11-6ubuntu2.1+esm1
- Installed package : gnupg_1.4.20-1ubuntu3.3
- Fixed package : gnupg_1.4.20-1ubuntu3.3+esm2
- Installed package : gnupg-agent_2.1.11-6ubuntu2.1
- Fixed package : gnupg-agent_2.1.11-6ubuntu2.1+esm1
- Installed package : gnupg2_2.1.11-6ubuntu2.1
- Fixed package : gnupg2_2.1.11-6ubuntu2.1+esm1
- Installed package : gpgv_1.4.20-1ubuntu3.3
- Fixed package : gpgv_1.4.20-1ubuntu3.3+esm2

168312 - Ubuntu 16.04 ESM : GnuTLS vulnerability (USN-5750-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5750-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5750-1>

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-2021-4209
XREF USN:5750-1

Plugin Information

Published: 2022/11/30, 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.

- Installed package : libgnutls-openssl27_3.4.10-4ubuntu1.4
- Fixed package : libgnutls-openssl27_3.4.10-4ubuntu1.9+esm1

- Installed package : libgnutls30_3.4.10-4ubuntu1.4
- Fixed package : libgnutls30_3.4.10-4ubuntu1.9+esm1

165716 - Ubuntu 16.04 ESM : Graphite2 vulnerability (USN-5657-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5657-1 advisory.

It was discovered that Graphite2 mishandled specially crafted files. An attacker could possibly use this issue to cause a denial of service or other unspecified impact.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5657-1>

Solution

Update the affected libgraphite2-3 and / or libgraphite2-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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-2018-7999](#)
XREF USN:5657-1

Plugin Information

Published: 2022/10/05, 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.

- Installed package : libgraphite2-3_1.3.10-0ubuntu0.16.04.1
- Fixed package : libgraphite2-3_1.3.10-0ubuntu0.16.04.1+esm1

[163267 - Ubuntu 16.04 ESM : HTTP-Daemon vulnerability \(USN-5520-2\)](#)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5520-2 advisory.

USN-5520-1 fixed a vulnerability in HTTP-Daemon. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5520-2>

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:5520-2

Plugin Information

Published: 2022/07/18, Modified: 2024/10/29

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 : libhttp-daemon-perl_6.01-1
- Fixed package : libhttp-daemon-perl_6.01-1ubuntu0.16.04~esm1

168234 - Ubuntu 16.04 ESM : HarfBuzz vulnerability (USN-5746-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5746-1 advisory.

Behzad Najarpour Jabbari discovered that HarfBuzz incorrectly handled certain inputs. 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-5746-1>

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-2015-9274
XREF USN:5746-1

Plugin Information

Published: 2022/11/28, 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.

- Installed package : libharfbuzz-icu0_1.0.1-1ubuntu0.1
- Fixed package : libharfbuzz-icu0_1.0.1-1ubuntu0.1+esm1
- Installed package : libharfbuzz0b_1.0.1-1ubuntu0.1
- Fixed package : libharfbuzz0b_1.0.1-1ubuntu0.1+esm1

159107 - Ubuntu 16.04 ESM : ImageMagick vulnerabilities (USN-5335-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5335-1 advisory.

It was discovered that ImageMagick incorrectly handled certain values when processing XPM image data or large images. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or possibly execute code with the privileges of the user invoking the program. (CVE-2020-19667, CVE-2017-13144)

Suhwan Song discovered that ImageMagick incorrectly handled memory when processing PNG,PALM,MIFF image data. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or possibly execute code with the privileges of the user invoking the program. (CVE-2020-25664, CVE-2020-25665, CVE-2020-25674, CVE-2020-27753)

Suhwan Song discovered that ImageMagick incorrectly handled certain values when processing image data. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. (CVE-2020-25676, CVE-2020-27750, CVE-2020-27760, CVE-2020-27762, CVE-2020-27766, CVE-2020-27770)

Zhang Xiaohui discovered that ImageMagick incorrectly handled certain values when processing image data.

If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. (CVE-2021-20176, CVE-2021-20241, CVE-2021-20243)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5335-1>

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-2017-13144
CVE	CVE-2020-19667
CVE	CVE-2020-25664
CVE	CVE-2020-25665
CVE	CVE-2020-25674
CVE	CVE-2020-25676

CVE	CVE-2020-27750
CVE	CVE-2020-27753
CVE	CVE-2020-27760
CVE	CVE-2020-27762
CVE	CVE-2020-27766
CVE	CVE-2020-27770
CVE	CVE-2021-20176
CVE	CVE-2021-20241
CVE	CVE-2021-20243
XREF	USN:5335-1
XREF	IAVB:2020-B-0042-S

Plugin Information

Published: 2022/03/21, 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.

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm2
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm2
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm2
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm2
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm2
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm2

163467 - Ubuntu 16.04 ESM : ImageMagick vulnerabilities (USN-5534-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5534-1 advisory.

It was discovered that ImageMagick incorrectly handled certain values. If a user were tricked into processing a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. (CVE-2022-32545, CVE-2022-32546)

It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into processing a specially crafted image file, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact. (CVE-2022-32547)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5534-1>

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-2022-32545
CVE	CVE-2022-32546
CVE	CVE-2022-32547
XREF	USN:5534-1

Plugin Information

Published: 2022/07/26, 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.

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.16+esm4
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.16+esm4
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.16+esm4
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm4
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.16+esm4
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.16+esm4

163520 - Ubuntu 16.04 ESM : Intel Microcode vulnerabilities (USN-5535-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5535-1 advisory.

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 implement sufficient control flow management. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-0127)

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)

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)

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)

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 (system crash). (CVE-2021-33120)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5535-1>

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-2022-21125
CVE	CVE-2022-21127
CVE	CVE-2022-21151
CVE	CVE-2022-21166
XREF	USN:5535-1

Plugin Information

Published: 2022/07/28, 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.

- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20220510.0ubuntu0.16.04.1+esm1

165690 - Ubuntu 16.04 ESM : JACK vulnerability (USN-5656-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5656-1 advisory.

Joseph Yasi discovered that JACK incorrectly handled the closing of a socket in certain conditions. An attacker could potentially 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-5656-1>

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

7.3 (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-2019-13351
XREF USN:5656-1

Plugin Information

Published: 2022/10/05, Modified: 2025/02/20

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 : libjack-jackd2-0_1.9.10+20150825git1ed50c92~dfsg-1ubuntu1
- Fixed package : libjack-jackd2-0_1.9.10+20150825git1ed50c92~dfsg-1ubuntu1+esm1

166558 - Ubuntu 16.04 ESM : Jinja2 vulnerability (USN-5701-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5701-1 advisory.

Yeting Li discovered that Jinja2 incorrectly handled certain 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-5701-1>

Solution

Update the affected python-jinja2 and / or python3-jinja2 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

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

5.0 (CVSS:2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS:2#E:POC/RL:OF/RC:C)

References

CVE-2020-28493
USN:5701-1

Plugin Information

Published: 2022/10/26, 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.

- Installed package : python3-jinja2_2.8-1
- Fixed package : python3-jinja2_2.8-1ubuntu0.1+esm1

163272 - Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5523-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5523-1 advisory.

It was discovered that LibTIFF was not properly performing checks to guarantee that allocated memory space existed, which could lead to a NULL pointer dereference via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0907, CVE-2022-0908)

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 behavior situation via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0909)

It was discovered that LibTIFF was not properly performing bounds checks, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2022-0924)

It was discovered that LibTIFF was not properly performing the calculation of data that would eventually be used as a reference for bounds checking operations, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2020-19131)

It was discovered that LibTIFF was not properly terminating a function execution when processing incorrect data, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2020-19144)

It was discovered that LibTIFF was not properly performing checks when setting the value for data later used as reference during memory access, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2022-22844)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5523-1>

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-2020-19131
CVE	CVE-2020-19144
CVE	CVE-2022-0907
CVE	CVE-2022-0908
CVE	CVE-2022-0909
CVE	CVE-2022-0924
CVE	CVE-2022-22844
XREF	USN:5523-1

Plugin Information

Published: 2022/07/19, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm2

164890 - Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5604-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5604-1 advisory.

It was discovered that LibTIFF incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-2867, CVE-2022-2869)

It was discovered that LibTIFF incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2868)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5604-1>

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-2022-2867
CVE	CVE-2022-2868
CVE	CVE-2022-2869
XREF	USN:5604-1

Plugin Information

Published: 2022/09/08, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm3

170966 - Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5841-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5841-1 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. This issue was only fixed in Ubuntu 14.04 ESM. (CVE-2019-14973, CVE-2019-17546, CVE-2020-35523, CVE-2020-35524, CVE-2022-3970)

It was discovered that LibTIFF was incorrectly accessing a data structure when processing data with the tiffcrop tool, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-48281)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5841-1>

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-2019-14973
CVE	CVE-2019-17546
CVE	CVE-2020-35523
CVE	CVE-2020-35524
CVE	CVE-2022-3970
CVE	CVE-2022-48281
XREF	USN:5841-1

Plugin Information

Published: 2023/02/02, 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.

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8+esm9

160213 - Ubuntu 16.04 ESM : Libcroco vulnerabilities (USN-5389-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5389-1 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. (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-5389-1>

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:5389-1

Plugin Information

Published: 2022/04/26, 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.

- Installed package : libcroco3_0.6.11-1
- Fixed package : libcroco3_0.6.11-1ubuntu0.1~esm1

153514 - Ubuntu 16.04 ESM : Libgcrypt vulnerabilities (USN-5080-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5080-2 advisory.

USN-5080-1 fixed several vulnerabilities in Libgcrypt. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5080-2>

Solution

Update the affected libgcrypt11-dev, libgcrypt20 and / or libgcrypt20-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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:5080-2

Plugin Information

Published: 2021/09/21, Modified: 2024/10/30

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 : libgcrypt20_1.6.5-2ubuntu0.5
- Fixed package : libgcrypt20_1.6.5-2ubuntu0.6+esm1

164326 - Ubuntu 16.04 ESM : Libxslt vulnerabilities (USN-5575-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5575-2 advisory.

USN-5575-1 fixed vulnerabilities in Libxslt. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5575-2>

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
XREF

CVE-2021-30560
USN:5575-2

Plugin Information

Published: 2022/08/22, Modified: 2024/10/29

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 : libxslt1.1_1.1.28-2.1ubuntu0.1
- Fixed package : libxslt1.1_1.1.28-2.1ubuntu0.3+esm1

168344 - Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5757-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5757-2 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 the video4linux driver for Empia based TV cards 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-2022-3239)

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-5757-2>

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-2022-3239
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:5757-2

Plugin Information

Published: 2022/12/02, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-200-generic for this advisory.

153942 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5022-3)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5022-3 advisory.

USN-5022-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5022-3>

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-2146
CVE	CVE-2021-2154
CVE	CVE-2021-2162
CVE	CVE-2021-2166
CVE	CVE-2021-2169
CVE	CVE-2021-2171
CVE	CVE-2021-2179
CVE	CVE-2021-2180
CVE	CVE-2021-2194
CVE	CVE-2021-2226
CVE	CVE-2021-2307
CVE	CVE-2021-2342
CVE	CVE-2021-2372
CVE	CVE-2021-2385
CVE	CVE-2021-2389
CVE	CVE-2021-2390
XREF	USN:5022-3
XREF	CEA-ID:CEA-2021-0025
XREF	IAVA:2021-A-0193-S
XREF	IAVA:2021-A-0333-S

Plugin Information

Published: 2021/10/08, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.35-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.35-0ubuntu0.16.04.1+esm1

154415 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5123-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5123-2 advisory.

USN-5123-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5123-2>

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
CVE	CVE-2021-35624
XREF	USN:5123-2
XREF	IAVA:2021-A-0487-S

Plugin Information

Published: 2021/10/26, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.36-0ubuntu0.16.04.1+esm1

- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.36-0ubuntu0.16.04.1+esm1

[157370 - Ubuntu 16.04 ESM : MySQL vulnerabilities \(USN-5270-2\)](#)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5270-2 advisory.

USN-5270-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also<https://ubuntu.com/security/notices/USN-5270-2>**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-2022-21245
CVE	CVE-2022-21270
CVE	CVE-2022-21303
CVE	CVE-2022-21304
CVE	CVE-2022-21344
CVE	CVE-2022-21367
XREF	USN:5270-2
XREF	IAVA:2022-A-0030-S

Plugin Information

Published: 2022/02/04, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.37-0ubuntu0.16.04.1+esm1

- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.37-0ubuntu0.16.04.1+esm1

166569 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5696-2)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5696-2 advisory.

USN-5696-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5696-2>

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-2022-21608
CVE	CVE-2022-21617
XREF	USN:5696-2

Plugin Information

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

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.40-0ubuntu0.16.04.1+esm1

- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.40-0ubuntu0.16.04.1+esm1

163561 - Ubuntu 16.04 ESM : MySQL vulnerability (USN-5537-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5537-2 advisory.

USN-5537-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5537-2>

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

6.1 (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-2022-21515
XREF	USN:5537-2

Plugin Information

Published: 2022/07/29, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.39-0ubuntu0.16.04.1+esm2
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.39-0ubuntu0.16.04.1+esm2

170561 - Ubuntu 16.04 ESM : MySQL vulnerability (USN-5823-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5823-2 advisory.

USN-5823-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5823-2>

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

6.1 (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)

STIG Severity

I

References

CVE	CVE-2023-21840
XREF	USN:5823-2
XREF	IAVA:2023-A-0043-S

Plugin Information

Published: 2023/01/25, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.41-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.41-0ubuntu0.16.04.1+esm1

161670 - Ubuntu 16.04 ESM : NTFS-3G vulnerability (USN-5452-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5452-1 advisory.

It was discovered that NTFS-3G was incorrectly validating NTFS metadata in its ntfsck tool by not performing boundary checks. A local attacker could possibly use this issue to cause a denial of service 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-5452-1>

Solution

Update the affected ntfs-3g and / or ntfs-3g-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

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-2021-46790
XREF	USN:5452-1

Plugin Information

Published: 2022/05/30, 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.

- Installed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.3+esm2

166940 - Ubuntu 16.04 ESM : NTFS-3G vulnerability (USN-5711-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5711-2 advisory.

USN-5711-1 fixed a vulnerability in NTFS-3G. This update provides the corresponding update for Ubuntu 14.04 ESM Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5711-2>

Solution

Update the affected ntfs-3g and / or ntfs-3g-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-40284
XREF	USN:5711-2

Plugin Information

Published: 2022/11/03, Modified: 2024/10/29

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 : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.3+esm4

150948 - Ubuntu 16.04 ESM : OpenEXR vulnerabilities (USN-4996-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4996-2 advisory.

USN-4996-1 fixed several vulnerabilities in OpenEXR. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-4996-2>

Solution

Update the affected libopenexr-dev, libopenexr22 and / or openexr 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

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-2021-3598
CVE	CVE-2021-3605
CVE	CVE-2021-20296
CVE	CVE-2021-23215
CVE	CVE-2021-26260
XREF	USN:4996-2

Plugin Information

Published: 2021/06/22, Modified: 2024/10/29

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 : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.6+esm1

166010 - Ubuntu 16.04 ESM : OpenSSH vulnerability (USN-5666-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

11/2/25, 1:18 AM

Photographer

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5666-1 advisory.

It was discovered that OpenSSH incorrectly handled certain helper programs. An attacker could possibly use this issue to 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-5666-1>

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

6.1 (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:O/RC:C)

STIG Severity

I

References

CVE	CVE-2021-41617
XREF	USN:5666-1
XREF	IAVA:2021-A-0474-S

Plugin Information

Published: 2022/10/11, 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.

- Installed package : openssh-client_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-client_1:7.2p2-4ubuntu2.10+esm2
- Installed package : openssh-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-server_1:7.2p2-4ubuntu2.10+esm2
- Installed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm2

152868 - Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-5051-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5051-2 advisory.

USN-5051-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5051-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

5.8 (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)

STIG Severity

I

References

CVE	CVE-2021-3712
XREF	USN:5051-2
XREF	IAVA:2021-A-0395-S

Plugin Information

Published: 2021/08/26, Modified: 2024/10/29

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 : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm1
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm1

158937 - Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-5328-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5328-2 advisory.

USN-5328-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5328-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl 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)

STIG Severity

I

References

CVE	CVE-2022-0778
XREF	USN:5328-2
XREF	IAVA:2022-A-0121-S

Plugin Information

Published: 2022/03/15, Modified: 2024/10/29

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 : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm2
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm2

166014 - Ubuntu 16.04 ESM : PCRE vulnerabilities (USN-5665-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5665-1 advisory.

It was discovered that PCRE incorrectly handled certain regular expressions. A remote attacker could use this issue to cause applications using PCRE to crash, resulting in a denial of service. (CVE-2017-6004)

It was discovered that PCRE incorrectly handled certain Unicode encoding. A remote attacker could use this issue to cause applications using PCRE to crash, resulting in a denial of service. (CVE-2017-7186)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5665-1>

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-2017-6004
CVE	CVE-2017-7186
XREF	USN:5665-1

Plugin Information

Published: 2022/10/11, 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.

- Installed package : libpcre16-3_2:8.38-3.1
- Fixed package : libpcre16-3_2:8.38-3.1ubuntu0.1~esm2

152178 - Ubuntu 16.04 ESM : QPFD vulnerabilities (USN-5026-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5026-2 advisory.

USN-5026-1 fixed several vulnerabilities in QPFD. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5026-2>

Solution

Update the affected libqpdf-dev, libqpdf21 and / or qpdf 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:5026-2

Plugin Information

Published: 2021/08/02, Modified: 2024/10/29

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 : libqpdf21_8.0.2-3~16.04.1
- Fixed package : libqpdf21_8.0.2-3~16.04.1+esm1

- Installed package : qpdf_8.0.2-3~16.04.1
- Fixed package : qpdf_8.0.2-3~16.04.1+esm1

161480 - Ubuntu 16.04 ESM : Rsyslog vulnerability (USN-5404-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5404-2 advisory.

USN-5404-1 addressed a vulnerability in Rsyslog. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5404-2>

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

References

CVE	CVE-2022-24903
XREF	USN:5404-2

Plugin Information

Published: 2022/05/24, Modified: 2024/08/29

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 : rsyslog_8.16.0-1ubuntu3
- Fixed package : rsyslog_8.16.0-1ubuntu3.1+esm2

153408 - Ubuntu 16.04 ESM : Squashfs-Tools vulnerabilities (USN-5078-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5078-2 advisory.

USN-5078-1 fixed several vulnerabilities in Squashfs-Tools. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5078-2>

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
CVE	CVE-2021-41072
XREF	USN:5078-2

Plugin Information

Published: 2021/09/15, Modified: 2024/10/29

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 : squashfs-tools_1:4.3-3ubuntu2.16.04.3
- Fixed package : squashfs-tools_1:4.3-3ubuntu2.16.04.3+esm1

176456 - Ubuntu 16.04 ESM : Sudo vulnerabilities (USN-6005-2)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6005-2 advisory.

USN-6005-1 fixed vulnerabilities in Sudo. This update provides the corresponding updates for Ubuntu 16.04 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-6005-2>

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:6005-2
XREF	IAVA:2023-A-0121-S

Plugin Information

Published: 2023/05/29, Modified: 2024/10/29

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 : sudo_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.10+esm2

170180 - Ubuntu 16.04 ESM : Sudo vulnerability (USN-5811-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5811-2 advisory.

USN-5811-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 16.04 ESM.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5811-2>

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22809
XREF	USN:5811-2

Exploitable With

Metasploit (true)

Plugin Information

Published: 2023/01/19, Modified: 2024/10/29

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 : sudo_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.10+esm1

161790 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5458-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5458-1 advisory.

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.

(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 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. (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)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5458-1>

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-2021-4193
CVE	CVE-2022-0213
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
XREF	USN:5458-1

Plugin Information

Published: 2022/06/02, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm5
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm5
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm5
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm5

161912 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5460-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5460-1 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. (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 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 was not properly performing bounds checks when executing spell suggestion commands, 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-2022-0943)

It was discovered that Vim was incorrectly performing bounds checks when processing invalid commands with composing characters in Ex mode, which could cause a buffer overflow. 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, 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-2022-1619)

It was discovered that Vim was not properly performing memory management when dealing with invalid regular expression patterns in buffers, which could cause a NULL pointer dereference. 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, 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-2022-1621)

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-5460-1>

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

7.9 (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-2022-0554
CVE	CVE-2022-0572
CVE	CVE-2022-0685
CVE	CVE-2022-0714
CVE	CVE-2022-0729
CVE	CVE-2022-0943
CVE	CVE-2022-1616
CVE	CVE-2022-1619
CVE	CVE-2022-1620
CVE	CVE-2022-1621
XREF	USN:5460-1

Plugin Information

Published: 2022/06/06, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm6
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm6
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm6
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm6

162625 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5498-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5498-1 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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5498-1>

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-2022-0413
CVE	CVE-2022-1629
CVE	CVE-2022-1733
CVE	CVE-2022-1735
CVE	CVE-2022-1785
CVE	CVE-2022-1796
CVE	CVE-2022-1851
CVE	CVE-2022-1898
XREF	USN:5498-1

Plugin Information

Published: 2022/06/30, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm8
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm8
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm8
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm8

162932 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5507-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5507-1 advisory.

It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the program to crash, use unexpected values, or execute arbitrary code. (CVE-2022-1968)

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-2022-1897, CVE-2022-1942)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5507-1>

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-2022-1897
CVE	CVE-2022-1942
CVE	CVE-2022-1968
XREF	USN:5507-1

Plugin Information

Published: 2022/07/08, Modified: 2024/08/29

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm10
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm10
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm10
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm10

163107 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5516-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5516-1 advisory.

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.

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

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

See Also

<https://ubuntu.com/security/notices/USN-5516-1>

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-2022-2000
CVE	CVE-2022-2207
CVE	CVE-2022-2210
XREF	USN:5516-1

Plugin Information

Published: 2022/07/14, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm11
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm11
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm11
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm11

167513 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5723-1)**Synopsis**

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5723-1 advisory.

It was discovered that Vim could be made to crash when searching specially crafted patterns. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-1674)

It was discovered that there existed a NULL pointer dereference in Vim. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-1725)

It was discovered that there existed a buffer over-read in Vim when searching specially crafted patterns. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-2124)

It was discovered that there existed a heap buffer overflow in Vim when auto-indenting lisp. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-2125)

It was discovered that there existed an out of bounds read in Vim when performing spelling suggestions. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-2126)

It was discovered that Vim accessed invalid memory when executing specially crafted command line expressions. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. (CVE-2022-2175)

It was discovered that there existed an out-of-bounds read in Vim when auto-indenting lisp. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands.

(CVE-2022-2183)

It was discovered that Vim accessed invalid memory when terminal size changed. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. (CVE-2022-2206)

It was discovered that there existed a stack buffer overflow in Vim's spelldump. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-2304)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5723-1>

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-2022-1674
CVE	CVE-2022-1725
CVE	CVE-2022-2124
CVE	CVE-2022-2125
CVE	CVE-2022-2126
CVE	CVE-2022-2127
CVE	CVE-2022-2175
CVE	CVE-2022-2183
CVE	CVE-2022-2206
CVE	CVE-2022-2304
XREF	USN:5723-1
XREF	IAVB:2022-B-0049-S
XREF	IAVB:2023-B-0016-S

Plugin Information

Published: 2022/11/15, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm13
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm13
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm13

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm13

168642 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5775-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5775-1 advisory.

It was discovered that Vim uses freed memory in recursive substitution of specially crafted patterns. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-2345)

It was discovered that Vim makes illegal memory calls when patterns start with an illegal byte. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands.

(CVE-2022-2581)

It was discovered that Vim could be made to crash when parsing invalid line numbers. An attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-3099)

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

It was discovered that Vim uses an incorrect array index when window width is negative. A local attacker could possibly use this to crash Vim and cause denial of service. (CVE-2022-3324)

It was discovered that certain buffers could be sent to the wrong window. An attacker with local access could use this to send messages to the wrong window. (CVE-2022-3591)

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

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

See Also

<https://ubuntu.com/security/notices/USN-5775-1>

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-2022-2345
CVE	CVE-2022-2581
CVE	CVE-2022-3099
CVE	CVE-2022-3256
CVE	CVE-2022-3324
CVE	CVE-2022-3591

XREF	USN:5775-1
XREF	IAVB:2022-B-0049-S
XREF	IAVB:2022-B-0058-S
XREF	IAVB:2023-B-0016-S

Plugin Information

Published: 2022/12/12, 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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm14
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm14
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm14
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm14

162514 - Ubuntu 16.04 ESM : Vim vulnerability (USN-5492-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5492-1 advisory.

It was discovered that Vim incorrectly handled memory when opening and searching the contents of certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to 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-5492-1>

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-2022-2042
XREF	USN:5492-1

Plugin Information

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm7
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm7
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm7
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm7

163468 - Ubuntu 16.04 ESM : Vim vulnerability (USN-5533-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5533-1 advisory.

It was discovered that Vim incorrectly handled memory access. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the corruption of sensitive information, a crash, or 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-5533-1>

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-2022-2129
XREF	USN:5533-1

Plugin Information

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm12
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm12
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm12
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm12

161171 - Ubuntu 16.04 ESM : Vorbis vulnerabilities (USN-5420-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5420-1 advisory.

It was discovered that Vorbis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2017-14160, CVE-2018-10392, CVE-2018-10393)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5420-1>

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-2017-14160
CVE	CVE-2018-10392
CVE	CVE-2018-10393
XREF	USN:5420-1

Plugin Information

Published: 2022/05/13, 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.

```
- Installed package : libvorbis0a_1.3.5-3ubuntu0.2
- Fixed package : libvorbis0a_1.3.5-3ubuntu0.2+esm1

- Installed package : libvorbisenc2_1.3.5-3ubuntu0.2
- Fixed package : libvorbisenc2_1.3.5-3ubuntu0.2+esm1

- Installed package : libvorbisfile3_1.3.5-3ubuntu0.2
- Fixed package : libvorbisfile3_1.3.5-3ubuntu0.2+esm1
```

167272 - Ubuntu 16.04 ESM : WavPack vulnerability (USN-5721-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5721-1 advisory.

It was discovered that WavPack was not properly performing checks when dealing with memory. If a user were tricked into decompressing a specially crafted WavPack Audio File, an attacker could possibly use this issue to cause the WavPack decompressor 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-5721-1>

Solution

Update the affected libwvpack-dev, libwvpack1 and / or wavpack packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-2476
XREF	USN:5721-1

Plugin Information

Published: 2022/11/10, 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.

```
- Installed package : libwvpack1_4.75.2-2ubuntu0.2
- Fixed package : libwvpack1_4.75.2-2ubuntu0.2+esm1
```

165662 - Ubuntu 16.04 ESM : Wayland vulnerability (USN-5614-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5614-2 advisory.

USN-5614-1 fixed a vulnerability in Wayland. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5614-2>

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:5614-2

Plugin Information

Published: 2022/10/05, Modified: 2024/10/29

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 : libwayland-client0_1.12.0-1~ubuntu16.04.3
- Fixed package : libwayland-client0_1.12.0-1~ubuntu16.04.3+esm1
- Installed package : libwayland-cursor0_1.12.0-1~ubuntu16.04.3
- Fixed package : libwayland-cursor0_1.12.0-1~ubuntu16.04.3+esm1
- Installed package : libwayland-server0_1.12.0-1~ubuntu16.04.3
- Fixed package : libwayland-server0_1.12.0-1~ubuntu16.04.3+esm1

163055 - Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5510-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5510-2 advisory.

USN-5510-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5510-2>

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:5510-2

Plugin Information

Published: 2022/07/12, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm2
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm1
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm1

153406 - Ubuntu 16.04 ESM : curl vulnerabilities (USN-5079-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5079-2 advisory.

USN-5079-1 fixed several vulnerabilities in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5079-2>

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/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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-2021-22946
CVE	CVE-2021-22947
XREF	USN:5079-2

Plugin Information

Published: 2021/09/15, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm1
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm1

162691 - Ubuntu 16.04 ESM : curl vulnerabilities (USN-5499-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5499-1 advisory.

Florian Kohnhuser discovered that curl incorrectly handled returning a TLS servers 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 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-5499-1>

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

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2022-27781
CVE	CVE-2022-32208
XREF	USN:5499-1
XREF	IAVA:2022-A-0224-S
XREF	IAVA:2022-A-0255-S

Plugin Information

Published: 2022/07/01, 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.

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm4

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm4

171954 - Ubuntu 16.04 ESM : curl vulnerabilities (USN-5894-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5894-1 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. This issue was only fixed in Ubuntu 14.04 ESM. (CVE-2021-22898, CVE-2021-22925)

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-5894-1>

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)

STIG Severity

I

References

CVE	CVE-2021-22898
CVE	CVE-2021-22925
CVE	CVE-2022-43552
XREF	USN:5894-1
XREF	IAVA:2023-A-0008-S
XREF	IAVA:2021-A-0352-S

Plugin Information

Published: 2023/02/28, 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.

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm7
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm7

156918 - Ubuntu 16.04 ESM : curl vulnerability (USN-5021-2)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5021-2 advisory.

USN-5021-1 fixed vulnerabilities in curl. This update provides the corresponding updates for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5021-2>

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)

STIG Severity

I

References

CVE	CVE-2021-22898
CVE	CVE-2021-22925
XREF	USN:5021-2
XREF	IAVA:2021-A-0437-S
XREF	IAVA:2021-A-0352-S

Plugin Information

Published: 2022/01/20, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm3
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm3

165525 - Ubuntu 16.04 ESM : libXi vulnerabilities (USN-5646-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5646-1 advisory.

Tobias Stoeckmann discovered that libXi did not properly manage memory when handling X server responses. A remote attacker could use this issue to cause libXi 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-5646-1>

Solution

Update the affected libxi-dev and / or libxi6 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-2016-7945
CVE	CVE-2016-7946
XREF	USN:5646-1

Plugin Information

Published: 2022/09/28, 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.

- Installed package : libxi6_2:1.7.6-1
- Fixed package : libxi6_2:1.7.6-1ubuntu0.1~esm1

164012 - Ubuntu 16.04 ESM : libcdio vulnerabilities (USN-5558-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5558-1 advisory.

Zhao Liang discovered that libcdio was not properly performing memory management operations when processing ISO files, which could result in a heap buffer overflow or in a NULL pointer dereference. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service. (CVE-2017-18198, CVE-2017-18199)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5558-1>

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-2017-18198
CVE	CVE-2017-18199
XREF	USN:5558-1

Plugin Information

Published: 2022/08/10, 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.

- Installed package : libcdio-cdda1_0.83-4.2ubuntu1
- Fixed package : libcdio-cdda1_0.83-4.2ubuntu1+esm1
- Installed package : libcdio-paranoia1_0.83-4.2ubuntu1
- Fixed package : libcdio-paranoia1_0.83-4.2ubuntu1+esm1
- Installed package : libcdio13_0.83-4.2ubuntu1
- Fixed package : libcdio13_0.83-4.2ubuntu1+esm1

163922 - Ubuntu 16.04 ESM : libjpeg-turbo vulnerabilities (USN-5553-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5553-1 advisory.

It was discovered that libjpeg-turbo was not properly handling EOF characters, which could lead to excessive memory consumption through the execution of a large loop. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-11813)

It was discovered that libjpeg-turbo was not properly performing bounds check operations, which could lead to a heap-based buffer overread. If a user or automated 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 14.04 ESM. (CVE-2018-14498)

It was discovered that libjpeg-turbo was not properly limiting the amount of main memory being consumed by the system during decompression or multi-pass compression operations, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-14152)

It was discovered that libjpeg-turbo was not properly setting variable sizes when performing certain kinds of encoding operations, which could lead to a stack-based buffer overflow. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service. (CVE-2020-17541)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5553-1>

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-2018-14498
CVE	CVE-2020-14152
CVE	CVE-2020-17541
XREF	USN:5553-1

Plugin Information

Published: 2022/08/09, 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.

- Installed package : `libjpeg-turbo8_1.4.2-0ubuntu3.1`
- Fixed package : `libjpeg-turbo8_1.4.2-0ubuntu3.4+esm1`

168279 - Ubuntu 16.04 ESM : libsamplerate vulnerability (USN-5749-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5749-1 advisory.

Erik de Castro Lopo and Agostino Sarubbo discovered that libsamplerate did not properly perform bounds checking. If a user were tricked into processing a specially crafted audio file, 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-5749-1>

Solution

Update the affected libsamplerate0, libsamplerate0-dev and / or samplerate-programs 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-2017-7697
XREF	USN:5749-1

Plugin Information

Published: 2022/11/29, 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.

- Installed package : libsamplerate0_0.1.8-8
- Fixed package : libsamplerate0_0.1.8-8ubuntu0.1~esm1

152144 - Ubuntu 16.04 ESM : libsndfile vulnerability (USN-5025-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5025-2 advisory.

USN-5025-1 fixed a vulnerability in libsndfile. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5025-2>

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:5025-2

Plugin Information

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 : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.3+esm1

160977 - Ubuntu 16.04 ESM : libsndfile vulnerability (USN-5409-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5409-1 advisory.

It was discovered that libsndfile was incorrectly performing memory management operations and incorrectly using buffers 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5409-1>

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
XREF	USN:5409-1

Plugin Information

Published: 2022/05/11, 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.

- Installed package : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.3+esm2

162173 - Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5477-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5477-1 advisory.

Hosein Askari discovered that ncurses was incorrectly performing memory management operations when dealing with long filenames while writing structures into the file system. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2017-16879)

Chung-Yi Lin discovered that ncurses was incorrectly handling access to invalid memory areas when parsing terminfo or termcap entries where the user-name had invalid syntax. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-19211)

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.

(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. (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. (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. (CVE-2022-29458)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5477-1>

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-2017-16879
CVE	CVE-2018-19211
CVE	CVE-2019-17594
CVE	CVE-2019-17595
CVE	CVE-2021-39537
CVE	CVE-2022-29458
XREF	USN:5477-1

Plugin Information

Published: 2022/06/14, 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.

- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm2
- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm2
- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm2
- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm2
- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm2
- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm2

168509 - Ubuntu 16.04 ESM : protobuf vulnerabilities (USN-5769-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5769-1 advisory.

It was discovered that protobuf did not properly manage memory when serializing large messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2015-5237)

It was discovered that protobuf 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. (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-5769-1>

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-2015-5237
CVE	CVE-2022-1941
XREF	USN:5769-1

Plugin Information

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 : libprotobuf-lite9v5_2.6.1-1.3
- Fixed package : libprotobuf-lite9v5_2.6.1-1.3ubuntu0.1~esm2

- Installed package : libprotobuf9v5_2.6.1-1.3
- Fixed package : libprotobuf9v5_2.6.1-1.3ubuntu0.1~esm2

162171 - Ubuntu 16.04 ESM : rsync vulnerability (USN-5359-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5359-2 advisory.

USN-5359-1 fixed vulnerabilities in rsync. This update provides the corresponding updates for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5359-2>

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
XREF

[CVE-2018-25032](#)

USN:5359-2

Plugin Information

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 : rsync_3.1.1-3ubuntu1.2
- Fixed package : rsync_3.1.1-3ubuntu1.3+esm1

158162 - Ubuntu 16.04 ESM : snapd vulnerabilities (USN-5292-3)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5292-3 advisory.

USN-5292-1 fixed several vulnerabilities in snapd. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5292-3>

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 (CVSS:2.0/AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS:2.0/EP:POC/RL:OF/RC:C)

References

CVE	CVE-2021-3155
CVE	CVE-2021-4120
CVE	CVE-2021-44730
CVE	CVE-2021-44731
XREF	USN:5292-3

Plugin Information

Published: 2022/02/18, Modified: 2024/10/29

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 : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.54.3+16.04~esm2
- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.54.3+16.04~esm2

151835 - Ubuntu 16.04 ESM : systemd vulnerabilities (USN-5013-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5013-2 advisory.

USN-5013-1 fixed several vulnerabilities in systemd. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5013-2>

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:5013-2
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/20, Modified: 2024/10/29

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 : libpam-systemd_229-4ubuntu21.16
- Fixed package : libpam-systemd_229-4ubuntu21.31+esm1
- Installed package : libsystemd0_229-4ubuntu21.16
- Fixed package : libsystemd0_229-4ubuntu21.31+esm1
- Installed package : libudev1_229-4ubuntu21.16
- Fixed package : libudev1_229-4ubuntu21.31+esm1
- Installed package : systemd_229-4ubuntu21.16
- Fixed package : systemd_229-4ubuntu21.31+esm1
- Installed package : systemd-sysv_229-4ubuntu21.16
- Fixed package : systemd-sysv_229-4ubuntu21.31+esm1
- Installed package : udev_229-4ubuntu21.16
- Fixed package : udev_229-4ubuntu21.31+esm1

158987 - Ubuntu 16.04 ESM : tcpdump vulnerabilities (USN-5331-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5331-1 advisory.

It was discovered that tcpdump incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2018-16301)

It was discovered that tcpdump incorrectly handled certain captured data. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-8037)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5331-1>

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/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: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:5331-1
XREF	IAVA:2021-A-0202-S

Plugin Information

Published: 2022/03/16, 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.

- Installed package : tcpdump_4.9.2-0ubuntu0.16.04.1
- Fixed package : tcpdump_4.9.3-0ubuntu0.16.04.1+esm1

162221 - Ubuntu 16.04 ESM : util-linux vulnerability (USN-5478-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5478-1 advisory.

Christian Moch and Michael Gruhn discovered that the libblkid library of util-linux did not properly manage memory under certain circumstances. A local attacker could possibly use this issue

to cause denial of service by consuming all memory through a specially crafted MSDOS partition table.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5478-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.6 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.0 (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-2016-5011
XREF	USN:5478-1

Plugin Information

Published: 2022/06/15, 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.

- Installed package : bsutils_1:2.27.1-6ubuntu3.6
- Fixed package : bsutils_1:2.27.1-6ubuntu3.10+esm2
- Installed package : libblkid1_2.27.1-6ubuntu3.6
- Fixed package : libblkid1_2.27.1-6ubuntu3.10+esm2
- Installed package : libfdisk1_2.27.1-6ubuntu3.6
- Fixed package : libfdisk1_2.27.1-6ubuntu3.10+esm2
- Installed package : libmount1_2.27.1-6ubuntu3.6
- Fixed package : libmount1_2.27.1-6ubuntu3.10+esm2
- Installed package : libsmartcols1_2.27.1-6ubuntu3.6
- Fixed package : libsmartcols1_2.27.1-6ubuntu3.10+esm2
- Installed package : libuuid1_2.27.1-6ubuntu3.6
- Fixed package : libuuid1_2.27.1-6ubuntu3.10+esm2

```
- Installed package : mount_2.27.1-6ubuntu3.6
- Fixed package : mount_2.27.1-6ubuntu3.10+esm2

- Installed package : util-linux_2.27.1-6ubuntu3.6
- Fixed package : util-linux_2.27.1-6ubuntu3.10+esm2

- Installed package : uuid-runtime_2.27.1-6ubuntu3.6
- Fixed package : uuid-runtime_2.27.1-6ubuntu3.10+esm2
```

159361 - Ubuntu 16.04 ESM : zlib vulnerability (USN-5355-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5355-2 advisory.

USN-5355-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5355-2>

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:5355-2

Plugin Information

Published: 2022/03/31, Modified: 2024/10/29

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 : zlib1g_1:1.2.8.dfsg-2ubuntu4.1
- Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3+esm1
```

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: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

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm6
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm6

- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.11+esm6
- Installed package : libcurlsgc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsgc1_2.1.3-4ubuntu0.11+esm6
- Installed package : libcurlimage2_2.1.3-4ubuntu0.7
- Fixed package : libcurlimage2_2.1.3-4ubuntu0.11+esm6
- Installed package : libcurlsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsmime1_2.1.3-4ubuntu0.11+esm6
- Installed package : libcurlppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlppdc1_2.1.3-4ubuntu0.11+esm6

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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20240514.0ubuntu0.16.04.1+esm1

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: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

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 : less_481-2.1ubuntu0.2
- Fixed package : less_481-2.1ubuntu0.2+esm1

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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20250512.0ubuntu0.16.04.1+esm1

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

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_2.52.2-1ubuntu0.3
- Fixed package : gir1.2-soup-2.4_2.52.2-1ubuntu0.3+esm3
- Installed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3+esm3
- Installed package : libsoup2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup2.4-1_2.52.2-1ubuntu0.3+esm3

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

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 : libvpx3_1.5.0-2ubuntu1
- Fixed package : libvpx3_1.5.0-2ubuntu1.1+esm4

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

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_1.13.1-2ubuntu0.16.04.2
- Fixed package : python3-urllib3_1.13.1-2ubuntu0.16.04.4+esm3

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 (CVSS2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.4 (CVSS2#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

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 : amd64-microcode_3.20180524.1~ubuntu0.16.04.2
- Fixed package : amd64-microcode_3.20191021.1+really3.20180524.1~ubuntu0.16.04.2+esm3

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/VC:H/Vl:H/VA: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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20241112.0ubuntu0.16.04.1+esm1

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: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

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_1.13.1-2ubuntu0.16.04.2
- Fixed package : python3-urllib3_1.13.1-2ubuntu0.16.04.4+esm2

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/R:L/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-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_2.52.2-1ubuntu0.3
- Fixed package : gir1.2-soup-2.4_2.52.2-1ubuntu0.3+esm5
- Installed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup-gnome2.4-1_2.52.2-1ubuntu0.3+esm5

- Installed package : libsoup2.4-1_2.52.2-1ubuntu0.3
- Fixed package : libsoup2.4-1_2.52.2-1ubuntu0.3+esm5

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

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 : libapr1_1.5.2-3
- Fixed package : libapr1_1.5.2-3ubuntu0.1~esm2

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/V:C:H/V:I: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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20240813.0ubuntu0.16.04.1+esm2

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: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

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 : nano_2.5.3-2ubuntu2
- Fixed package : nano_2.5.3-2ubuntu2+esm1

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 Grosen 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/VC:N/VI:N/VA: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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20250211.0ubuntu0.16.04.1+esm1

211385 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : GD Graphics Library vulnerability (USN-7112-1)

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 host has packages installed that are affected by a vulnerability as referenced in the USN-7112-1 advisory.

It was discovered that the GD Graphics Library did not perform proper bounds checking while handling BMP and WebP files. If a user were tricked into opening a specially crafted file, an attacker could possibly 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-7112-1>

Solution

Update the affected libgd-dev, libgd-tools and / or libgd3 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-2021-40812
XREF	USN:7112-1

Plugin Information

Published: 2024/11/15, Modified: 2024/11/15

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 : libgd3_2.1.1-4ubuntu0.16.04.10
- Fixed package : libgd3_2.1.1-4ubuntu0.16.04.12+esm4

207976 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-7015-3)

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 host has packages installed that are affected by a vulnerability as referenced in the USN-7015-3 advisory.

USN-7015-1 fixed several vulnerabilities in Python. This update provides the corresponding updates for CVE-2023-27043 for python2.7 in Ubuntu 16.04 LTS,

Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS, and for python3.5 in Ubuntu 16.04 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-7015-3>

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
XREF	USN:7015-3

Plugin Information

Published: 2024/10/01, Modified: 2024/10/01

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm11
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm11
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm11
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm15
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm15
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm15
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm11
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm11
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm15
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm15

136608 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : APT vulnerability (USN-4359-1)

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-4359-1 advisory.

It was discovered that APT incorrectly handled certain filenames during package installation. If an attacker could provide a specially crafted package to be installed by the system administrator, this could cause APT to 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-4359-1>

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-2020-3810
XREF USN:4359-1

Plugin Information

Published: 2020/05/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : apt_1.2.29ubuntu0.1
- Fixed package : apt_1.2.32ubuntu0.1

- Installed package : apt-transport-https_1.2.29ubuntu0.1
- Fixed package : apt-transport-https_1.2.32ubuntu0.1

- Installed package : apt-utils_1.2.29ubuntu0.1
- Fixed package : apt-utils_1.2.32ubuntu0.1

- Installed package : libapt-inst2.0_1.2.29ubuntu0.1
- Fixed package : libapt-inst2.0_1.2.32ubuntu0.1

- Installed package : libapt-pkg5.0_1.2.29ubuntu0.1
- Fixed package : libapt-pkg5.0_1.2.32ubuntu0.1
```

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/NC:H/VI:H/VA: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_1.2.29ubuntu0.1
- Fixed package : apt_1.2.32ubuntu0.2
- Installed package : apt-transport-https_1.2.29ubuntu0.1
- Fixed package : apt-transport-https_1.2.32ubuntu0.2
- Installed package : apt-utils_1.2.29ubuntu0.1
- Fixed package : apt-utils_1.2.32ubuntu0.2
- Installed package : libapt-inst2.0_1.2.29ubuntu0.1
- Fixed package : libapt-inst2.0_1.2.32ubuntu0.2
- Installed package : libapt-pkg5.0_1.2.29ubuntu0.1
- Fixed package : libapt-pkg5.0_1.2.32ubuntu0.2

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_0.6.40-2ubuntu11.3
- Fixed package : accountsservice_0.6.40-2ubuntu11.6
- Installed package : libaccountsservice0_0.6.40-2ubuntu11.3
- Fixed package : libaccountsservice0_0.6.40-2ubuntu11.6

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_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.24
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.24
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.24
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.24

136730 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Bind vulnerabilities (USN-4365-1)

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-4365-1 advisory.

Lior Shafir, Yehuda Afek, and Anat Bremler-Barr discovered that Bind incorrectly limited certain fetches.

A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service, or possibly use Bind to perform a reflection attack. (CVE-2020-8616)

Tobias Klein discovered that Bind incorrectly handled checking TSIG validity. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly perform other attacks.

(CVE-2020-8617)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4365-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

7.7 (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)

STIG Severity

I

References

CVE	CVE-2020-8616
CVE	CVE-2020-8617
XREF	USN:4365-1
KREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.16

- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.16
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.16

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-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-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.17

- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.17
```

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

I

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-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.19

- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.19
```

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-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.18
- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.18

136029 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : CUPS vulnerabilities (USN-4340-1)**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-4340-1 advisory.

It was discovered that CUPS incorrectly handled certain language values. A local attacker could possibly use this issue to cause CUPS to crash, leading to a denial of service, or possibly obtain sensitive information. This issue only applied to Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 19.10. (CVE-2019-2228)

Stephan Zeisberg discovered that CUPS incorrectly handled certain malformed ppd files. A local attacker could possibly use this issue to execute arbitrary code. (CVE-2020-3898)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4340-1>

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

4.9 (CVSS2#AV:L/AC:L/Au:N/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-2228
CVE	CVE-2020-3898
XREF	USN:4340-1

Plugin Information

Published: 2020/04/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11
- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.11
- Installed package : libcurlcgi1_2.1.3-4ubuntu0.7
- Fixed package : libcurlcgi1_2.1.3-4ubuntu0.11
- Installed package : libcurlimage2_2.1.3-4ubuntu0.7
- Fixed package : libcurlimage2_2.1.3-4ubuntu0.11
- Installed package : libcurlsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsmime1_2.1.3-4ubuntu0.11
- Installed package : libcurlppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlppdc1_2.1.3-4ubuntu0.11

137556 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : DBus vulnerability (USN-4398-1)

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-4398-1 advisory.

Kevin Backhouse discovered that DBus incorrectly handled file descriptors. A local attacker could possibly use this issue to cause DBus 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-4398-1>

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

4.9 (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-2020-12049
XREF	USN:4398-1

Plugin Information

Published: 2020/06/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dbus_1.10.6-1ubuntu3.3
- Fixed package : dbus_1.10.6-1ubuntu3.6
- Installed package : dbus-x11_1.10.6-1ubuntu3.3
- Fixed package : dbus-x11_1.10.6-1ubuntu3.6
- Installed package : libdbus-1-3_1.10.6-1ubuntu3.3
- Fixed package : libdbus-1-3_1.10.6-1ubuntu3.6

138873 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Evolution Data Server vulnerability (USN-4429-1)

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-4429-1 advisory.

It was discovered that Evolution Data Server incorrectly handled STARTTLS when using SMTP and POP3. A remote attacker could possibly use this issue to perform a response injection 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-4429-1>

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

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-2020-14928
XREF-USN:4429-1

Plugin Information

Published: 2020/07/23, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : evolution-data-server_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server_3.18.5-1ubuntu1.3
- Installed package : evolution-data-server-common_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server-common_3.18.5-1ubuntu1.3
- Installed package : evolution-data-server-online-accounts_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server-online-accounts_3.18.5-1ubuntu1.3
- Installed package : libcamel-1.2-54_3.18.5-1ubuntu1.1
- Fixed package : libcamel-1.2-54_3.18.5-1ubuntu1.3
- Installed package : libbackend-1.2-10_3.18.5-1ubuntu1.1
- Fixed package : libbackend-1.2-10_3.18.5-1ubuntu1.3
- Installed package : libebook-1.2-16_3.18.5-1ubuntu1.1
- Fixed package : libebook-1.2-16_3.18.5-1ubuntu1.3
- Installed package : libebook-contacts-1.2-2_3.18.5-1ubuntu1.1
- Fixed package : libebook-contacts-1.2-2_3.18.5-1ubuntu1.3
- Installed package : libecal-1.2-19_3.18.5-1ubuntu1.1
- Fixed package : libecal-1.2-19_3.18.5-1ubuntu1.3
- Installed package : libedata-book-1.2-25_3.18.5-1ubuntu1.1
- Fixed package : libedata-book-1.2-25_3.18.5-1ubuntu1.3
- Installed package : libedata-cal-1.2-28_3.18.5-1ubuntu1.1
- Fixed package : libedata-cal-1.2-28_3.18.5-1ubuntu1.3
- Installed package : libedataserver-1.2-21_3.18.5-1ubuntu1.1
- Fixed package : libedataserver-1.2-21_3.18.5-1ubuntu1.3
- Installed package : libedataserverui-1.2-1_3.18.5-1ubuntu1.1
- Fixed package : libedataserverui-1.2-1_3.18.5-1ubuntu1.3

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_80.0.1+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_80.0.1+build1-0ubuntu0.16.04.1
```

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_80.0+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_80.0+build2-0ubuntu0.16.04.1

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 in to 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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_81.0+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_81.0+build2-0ubuntu0.16.04.1

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 in to 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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_85.0+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_85.0+build1-0ubuntu0.16.04.1
```

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

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_86.0+build3-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_86.0+build3-0ubuntu0.16.04.1
```

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_87.0+build3-0ubuntu0.16.04.2

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_87.0+build3-0ubuntu0.16.04.2
```

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-

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_88.0+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_88.0+build2-0ubuntu0.16.04.1

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_84.0.2+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_84.0.2+build1-0ubuntu0.16.04.1

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_2.6.1-0.1ubuntu2.3
- Fixed package : libfreetype6_2.6.1-0.1ubuntu2.5

137872 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : GLib Networking vulnerability (USN-4405-1)

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-4405-1 advisory.

It was discovered that glib-networking skipped hostname certificate verification if the application failed to specify the server identity. A remote attacker could use this to perform a person-in-the-middle attack and 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-4405-1>

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)

References

CVE [CVE-2020-13645](#)
XREF USN:4405-1

Plugin Information

Published: 2020/06/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : glib-networking_2.48.2-1~ubuntu16.04.1
- Fixed package : glib-networking_2.48.2-1~ubuntu16.04.2
- Installed package : glib-networking-common_2.48.2-1~ubuntu16.04.1
- Fixed package : glib-networking-common_2.48.2-1~ubuntu16.04.2
- Installed package : glib-networking-services_2.48.2-1~ubuntu16.04.1
- Fixed package : glib-networking-services_2.48.2-1~ubuntu16.04.2

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_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.7
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.7
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.7

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_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.8
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.8
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.8

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_2.02~beta2-36ubuntu3.20
- Fixed package : grub-common_2.02~beta2-36ubuntu3.26
- Installed package : grub-pc_2.02~beta2-36ubuntu3.20
- Fixed package : grub-pc_2.02~beta2-36ubuntu3.26
- Installed package : grub-pc-bin_2.02~beta2-36ubuntu3.20
- Fixed package : grub-pc-bin_2.02~beta2-36ubuntu3.26
- Installed package : grub2-common_2.02~beta2-36ubuntu3.20
- Fixed package : grub2-common_2.02~beta2-36ubuntu3.26

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_2.02~beta2-36ubuntu3.20
- Fixed package : grub-common_2.02~beta2-36ubuntu3.27
- Installed package : grub-pc_2.02~beta2-36ubuntu3.20
- Fixed package : grub-pc_2.02~beta2-36ubuntu3.27
- Installed package : grub-pc-bin_2.02~beta2-36ubuntu3.20
- Fixed package : grub-pc-bin_2.02~beta2-36ubuntu3.27
- Installed package : grub2-common_2.02~beta2-36ubuntu3.20
- Fixed package : grub2-common_2.02~beta2-36ubuntu3.27

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-2021-3498
XREF USN:4928-1

Plugin Information

Published: 2021/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : gstreamer1.0-plugins-good_1.8.3-1ubuntu0.4
- Fixed package : gstreamer1.0-plugins-good_1.8.3-1ubuntu0.5
- Installed package : gstreamer1.0-pulseaudio_1.8.3-1ubuntu0.4
- Fixed package : gstreamer1.0-pulseaudio_1.8.3-1ubuntu0.5
- Installed package : libgstreamer-plugins-good1.0-0_1.8.3-1ubuntu0.4
- Fixed package : libgstreamer-plugins-good1.0-0_1.8.3-1ubuntu0.5

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_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.13

- Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.13

- Installed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.13

- Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.13
```

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_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2

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_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.8

138999 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer vulnerabilities (USN-4434-1)

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-4434-1 advisory.

Ramin Farajpour Cami discovered that LibVNCServer incorrectly handled certain malformed unix socket names.

A remote attacker could exploit this with a crafted socket name, leading to a denial of service, or possibly execute arbitrary code. (CVE-2019-20839)

It was discovered that LibVNCServer did not properly access byte-aligned data. A remote attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2019-20840)

Christian Beier discovered that LibVNCServer incorrectly handled anonymous TLS connections. A remote attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service.

This issue only affected Ubuntu 20.04 LTS. (CVE-2020-14396)

It was discovered that LibVNCServer incorrectly handled region clipping. A remote attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service. (CVE-2020-14397)

It was discovered that LibVNCServer did not properly reset incorrectly terminated TCP connections. A remote attacker could possibly use this issue to cause an infinite loop, resulting in a denial of service.

(CVE-2020-14398)

It was discovered that LibVNCServer did not properly access byte-aligned data. A remote attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service. (CVE-2020-14399, CVE-2020-14400)

It was discovered that LibVNCServer incorrectly handled screen scaling on the server side. A remote attacker could use this issue to cause LibVNCServer to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-14401)

It was discovered that LibVNCServer incorrectly handled encodings. A remote attacker could use this issue to cause LibVNCServer to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2020-14402, CVE-2020-14403, CVE-2020-14404)

It was discovered that LibVNCServer incorrectly handled TextChat messages. A remote attacker could possibly use this issue to cause LibVNCServer to crash, resulting in a denial of service. (CVE-2020-14405)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4434-1>

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-2019-20839
CVE	CVE-2019-20840
CVE	CVE-2020-14396
CVE	CVE-2020-14397
CVE	CVE-2020-14398
CVE	CVE-2020-14399
CVE	CVE-2020-14400
CVE	CVE-2020-14401
CVE	CVE-2020-14402
CVE	CVE-2020-14403
CVE	CVE-2020-14404
CVE	CVE-2020-14405
XREF	USN:4434-1

Plugin Information

Published: 2020/07/27, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.3
- Fixed package : libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.5

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_0.9.10+dfsg-3ubuntu0.16.04.3
- Fixed package : libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.6
- Installed package : vino_3.8.1-0ubuntu9.2
- Fixed package : vino_3.8.1-0ubuntu9.4

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-122-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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-132-generic for this advisory.

139181 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4441-1)

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-4441-1 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 8.0.21 in Ubuntu 20.04 LTS. Ubuntu 16.04 LTS and Ubuntu 18.04 LTS have been updated to MySQL 5.7.31.

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-5-7-31.html>

<https://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-21.html>

<https://www.oracle.com/security-alerts/cpujul2020.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-4441-1>

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

6.3 (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-2020-14539
CVE	CVE-2020-14540
CVE	CVE-2020-14547
CVE	CVE-2020-14550
CVE	CVE-2020-14553
CVE	CVE-2020-14559
CVE	CVE-2020-14568
CVE	CVE-2020-14575
CVE	CVE-2020-14576
CVE	CVE-2020-14586
CVE	CVE-2020-14591
CVE	CVE-2020-14597
CVE	CVE-2020-14619
CVE	CVE-2020-14620
CVE	CVE-2020-14623
CVE	CVE-2020-14624
CVE	CVE-2020-14631
CVE	CVE-2020-14632
CVE	CVE-2020-14633
CVE	CVE-2020-14634
CVE	CVE-2020-14641

CVE	CVE-2020-14643
CVE	CVE-2020-14651
CVE	CVE-2020-14654
CVE	CVE-2020-14656
CVE	CVE-2020-14663
CVE	CVE-2020-14678
CVE	CVE-2020-14680
CVE	CVE-2020-14697
CVE	CVE-2020-14702
XREF	USN:4441-1

Plugin Information

Published: 2020/07/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.31-0ubuntu0.16.04.1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.31-0ubuntu0.16.04.1

137555 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerabilities (USN-4397-1)

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-4397-1 advisory.

It was discovered that NSS incorrectly handled the TLS State Machine. A remote attacker could possibly use this issue to cause NSS to hang, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 19.10. (CVE-2019-17023)

Cesar Pereida Garcia discovered that NSS incorrectly handled DSA key generation. A local attacker could possibly use this issue to perform a timing attack and recover DSA keys. (CVE-2020-12399)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4397-1>

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)

References

CVE	CVE-2019-17023
CVE	CVE-2020-12399

Plugin Information

Published: 2020/06/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.11
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.11

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_2:3.28.4-0ubuntu0.16.04.4

- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.13
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.13

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_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.14
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.14

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	CVE-2021-20305
XREF	USN:4906-1

Plugin Information

Published: 2021/04/14, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libhogweed4_3.2-1ubuntu0.16.04.1
- Fixed package : libhogweed4_3.2-1ubuntu0.16.04.2
- Installed package : libnettle6_3.2-1ubuntu0.16.04.1
- Fixed package : libnettle6_3.2-1ubuntu0.16.04.2

136028 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4339-1)

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-4339-1 advisory.

Brandon Perry discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. This issue only applied to Ubuntu 20.04 LTS. (CVE-2017-9111, CVE-2017-9113, CVE-2017-9115)

Tan Jie discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. This issue only applied to Ubuntu 20.04 LTS. (CVE-2018-1844)

Samuel Gro discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. (CVE-2020-11758, CVE-2020-11759, CVE-2020-11760, CVE-2020-11761, CVE-2020-11762, CVE-2020-11763, CVE-2020-11764)

It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service.
(CVE-2020-11765)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4339-1>

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-2017-9111
CVE	CVE-2017-9113
CVE	CVE-2017-9115
CVE	CVE-2018-18444
CVE	CVE-2020-11758
CVE	CVE-2020-11759
CVE	CVE-2020-11760
CVE	CVE-2020-11761
CVE	CVE-2020-11762
CVE	CVE-2020-11763
CVE	CVE-2020-11764
CVE	CVE-2020-11765
XREF	USN:4339-1

Plugin Information

Published: 2020/04/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.2

144746 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4676-1)

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-4676-1 advisory.

It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image 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-4676-1>

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-2020-16587
CVE	CVE-2020-16588
CVE	CVE-2020-16589
XREF	USN:4676-1

Plugin Information

Published: 2021/01/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.4

148295 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4900-1)

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-4900-1 advisory.

It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image 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-4900-1>

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

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-2021-3474
CVE	CVE-2021-3475
CVE	CVE-2021-3476
CVE	CVE-2021-3477
CVE	CVE-2021-3478
CVE	CVE-2021-3479
XREF	USN:4900-1

Plugin Information

Published: 2021/04/01, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.6

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_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.11

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_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.12

136401 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4352-1)**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-4352-1 advisory.

It was discovered that OpenLDAP incorrectly handled certain queries. A remote attacker could possibly use this issue to cause OpenLDAP 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-4352-1>

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)

STIG Severity

I

References

CVE	CVE-2020-12243
XREF	USN:4352-1
XREF	IAVB:2020-B-0028-S

Plugin Information

Published: 2020/05/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.8

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_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.10

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
XREF

[CVE-2021-27212](#)
USN:4744-1

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13

148011 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenSSL vulnerabilities (USN-4738-1)**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-4738-1 advisory.

Paul Kehrer discovered that OpenSSL incorrectly handled certain input lengths in EVP functions. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service.

(CVE-2021-23840)

Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer fields. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2021-23841)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4738-1>

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-2021-23840
CVE	CVE-2021-23841
XREF	USN:4738-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.19
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.19

143587 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenSSL vulnerability (USN-4662-1)**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-4662-1 advisory.

David Benjamin discovered that OpenSSL incorrectly handled comparing certificates containing a EDIPartyName name type. A remote attacker could possibly use this issue to cause OpenSSL 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-4662-1>

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

5.5 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:F/RL:O/RC:C)

STIG Severity

I

References

CVE	CVE-2020-1971
XREF	USN:4662-1
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.18
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.18

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_3.1.2-0ubuntu1.1`
- Fixed package : `python3-pil_3.1.2-0ubuntu1.5`

138872 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-4428-1)

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-4428-1 advisory.

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 12.04 ESM, Ubuntu 14.04 ESM, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-17514)

It was discovered that Python incorrectly handled certain TAR archives. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-20907)

It was discovered that incorrectly handled certain ZIP files. 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-2019-9674)

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 ESM, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-14422)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4428-1>

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-2019-17514
CVE	CVE-2019-20907
CVE	CVE-2019-9674
CVE	CVE-2020-14422
XREF	USN:4428-1
XREF	IAVA:2020-A-0340-S

Plugin Information

Published: 2020/07/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.12
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.12
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.12
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.11
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.11
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.11
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.12
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.12
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.11

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.11

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_2.0.14-1
- Fixed package : libraptor2-0_2.0.14-1ubuntu0.16.04.1

137353 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-4394-1)

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-4394-1 advisory.

It was discovered that SQLite incorrectly handled certain corrupted schemas. An attacker could possibly use this issue to cause a denial of service. This issue only

affected Ubuntu 18.04 LTS. (CVE-2018-8740)

It was discovered that SQLite incorrectly handled certain SELECT statements. An attacker could possibly use this issue to cause a denial of service. This issue was only addressed in Ubuntu 19.10.
(CVE-2019-19603)

It was discovered that SQLite incorrectly handled certain self-referential views. An attacker could possibly use this issue to cause a denial of service. This issue was only addressed in Ubuntu 19.10.
(CVE-2019-19645)

Henry Liu discovered that SQLite incorrectly handled certain malformed window-function queries. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-11655)

It was discovered that SQLite incorrectly handled certain string operations. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2020-13434)

It was discovered that SQLite incorrectly handled certain expressions. 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 19.10 and Ubuntu 20.04 LTS. (CVE-2020-13435)

It was discovered that SQLite incorrectly handled certain fts3 queries. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2020-13630)

It was discovered that SQLite incorrectly handled certain virtual table names. An attacker could possibly use this issue to cause a denial of service. This issue was only addressed in Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-13631)

It was discovered that SQLite incorrectly handled certain fts3 queries. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2020-13632)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4394-1>

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 (CVSS:2.0/AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS:2.0/POC/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2018-8740
CVE	CVE-2019-19603
CVE	CVE-2019-19645
CVE	CVE-2020-11655
CVE	CVE-2020-13434
CVE	CVE-2020-13435
CVE	CVE-2020-13630
CVE	CVE-2020-13631
CVE	CVE-2020-13632

XREF USN:4394-1
XREF IAVA:2020-A-0358-S

Plugin Information

Published: 2020/06/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5

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 (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-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 : libsmbclient_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libsmbclient_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.32

- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.32

```

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	CVE-2020-14303
XREF	USN:4454-1

Plugin Information

Published: 2020/08/11, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : lib smbclient_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : lib smbclient_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : lib wbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : lib wbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.29

- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.29
```

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

|

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_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libsmclient_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : libwbclient0_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : python-samba_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-common-bin_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-dsdb-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-libs_2:4.3.11+dfsg-0ubuntu0.16.04.34

- Installed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.28
- Fixed package : samba-vfs-modules_2:4.3.11+dfsg-0ubuntu0.16.04.34
```

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_0.2.52.5
- Fixed package : libwhoopsie0_0.2.52.5ubuntu0.5
- Installed package : whoopsie_0.2.52.5
- Fixed package : whoopsie_0.2.52.5ubuntu0.5

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_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.9
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.3
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.3

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	CVE-2020-14360
CVE	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_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.11
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.5
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.5

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

Plugin Output

tcp/0

```
- Installed package : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.10

- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.4

- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.4
```

137824 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-4402-1)

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-4402-1 advisory.

Marek Szlagor, Gregory Jefferis and Jeroen Ooms discovered that curl incorrectly handled certain credentials. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-8169)

It was discovered that curl incorrectly handled certain parameters. An attacker could possibly use this issue to overwrite a local file. (CVE-2020-8177)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4402-1>

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

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-2020-8169
CVE	CVE-2020-8177
XREF	USN:4402-1
XREF	IAVA:2020-A-0291-S

Plugin Information

Published: 2020/06/25, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.15

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.15

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. (CVE-2020-8286)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested 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_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.18
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.18

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_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19
```

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_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.16

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.16
```

136663 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : json-c vulnerability (USN-4360-1)

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-4360-1 advisory.

It was discovered that json-c incorrectly handled certain JSON 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-4360-1>

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-2020-12762
XREF-USN:4360-1

Plugin Information

Published: 2020/05/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libjson-c2_0.11-4ubuntu2
- Fixed package : libjson-c2_0.11-4ubuntu2.1

136964 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : json-c vulnerability (USN-4360-4)

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-4360-4 advisory.

USN-4360-1 fixed a vulnerability in json-c. The security fix introduced a memory leak that was reverted in USN-4360-2 and USN-4360-3. This update provides the correct fix update for CVE-2020-12762.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4360-4>

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-2020-12762
XREF	USN:4360-4

Plugin Information

Published: 2020/05/29, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libjson-c2_0.11-4ubuntu2
- Fixed package : libjson-c2_0.11-4ubuntu2.6
```

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:H/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 : libldb1_2:1.1.24-1ubuntu3.1
- Fixed package : libldb1_2:1.1.24-1ubuntu3.2
- Installed package : python-ldb_2:1.1.24-1ubuntu3.1
- Fixed package : python-ldb_2:1.1.24-1ubuntu3.2

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	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.beta19-2ubuntu0.16.04.1
- Fixed package : libcaca0_0.99.beta19-2ubuntu0.16.04.2

137554 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif vulnerabilities (USN-4396-1)**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-4396-1 advisory.

It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-0093, CVE-2020-0182)

It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a remote denial of service. (CVE-2020-0198)

It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information or cause a crash. (CVE-2020-13112)

It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. (CVE-2020-13113)

It was discovered libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-13114)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4396-1>

Solution

Update the affected libexif-dev and / or libexif12 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

References

CVE	CVE-2020-0093
CVE	CVE-2020-0182
CVE	CVE-2020-0198
CVE	CVE-2020-13112
CVE	CVE-2020-13113
CVE	CVE-2020-13114
XREF	USN:4396-1

Plugin Information

Published: 2020/06/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexif12_0.6.21-2
- Fixed package : libexif12_0.6.21-2ubuntu0.5

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	CVE-2025-40907
XREF	USN:7527-1

Plugin Information

Published: 2025/05/22, Modified: 2025/05/22

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 : libfcgi-perl_0.77-1build1
- Fixed package : libfcgi-perl_0.77-1ubuntu0.1~esm1

137296 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libjpeg-turbo vulnerability (USN-4386-1)

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-4386-1 advisory.

It was discovered that libjpeg-turbo incorrectly handled certain PPM files. An attacker could possibly use this issue to access 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-4386-1>

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:N/A:H)

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-13790
XREF	USN:4386-1

Plugin Information

Published: 2020/06/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libjpeg-turbo8_1.4.2-0ubuntu3.1
- Fixed package : libjpeg-turbo8_1.4.2-0ubuntu3.4

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_0.4.11-5ubuntu1
- Fixed package : libproxy1-plugin-gsettings_0.4.11-5ubuntu1.1
- Installed package : libproxy1-plugin-networkmanager_0.4.11-5ubuntu1
- Fixed package : libproxy1-plugin-networkmanager_0.4.11-5ubuntu1.1
- Installed package : libproxy1v5_0.4.11-5ubuntu1
- Fixed package : libproxy1v5_0.4.11-5ubuntu1.1

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-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_0.4.11-5ubuntu1
- Fixed package : libproxy1-plugin-gsettings_0.4.11-5ubuntu1.2
- Installed package : libproxy1-plugin-networkmanager_0.4.11-5ubuntu1
- Fixed package : libproxy1-plugin-networkmanager_0.4.11-5ubuntu1.2
- Installed package : libproxy1v5_0.4.11-5ubuntu1
- Fixed package : libproxy1v5_0.4.11-5ubuntu1.2

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_0.6.3-4.3ubuntu0.2
- Fixed package : libssh-4_0.6.3-4.3ubuntu0.6

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_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-6_2:1.6.3-1ubuntu2.2

- Installed package : libx11-data_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-data_2:1.6.3-1ubuntu2.2

- Installed package : libx11-xcb1_2:1.6.3-1ubuntu2.1
- Fixed package : libx11-xcb1_2:1.6.3-1ubuntu2.2
```

144012 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : lxml vulnerability (USN-4666-1)

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-4666-1 advisory.

It was discovered that lxml incorrectly handled certain HTML. An attacker could possibly use this issue to cross-site scripting (XSS) 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-4666-1>

Solution

Update the affected python-lxml and / or python3-lxml 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/Vl:H/Va:H/SC:N/SI:N/SA:N)

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

5.5 (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-2020-27783
XREF	USN:4666-1

Plugin Information

Published: 2020/12/09, Modified: 2024/09/19

Plugin Output

tcp/0

- Installed package : python3-lxml_3.5.0-1ubuntu0.1
- Fixed package : python3-lxml_3.5.0-1ubuntu0.2

144078 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : lxml vulnerability (USN-4666-2)

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-4666-2 advisory.

USN-4666-1 partially fixed a vulnerability in lxml, but an additional patch was needed. This update provides the corresponding additional patch in order to properly fix the vulnerability.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4666-2>

Solution

Update the affected python-lxml and / or python3-lxml packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.5 (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-2020-27783
XREF USN:4666-2

Plugin Information

Published: 2020/12/11, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : python3-lxml_3.5.0-1ubuntu0.1

- Fixed package : python3-lxml_3.5.0-1ubuntu0.3

148244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : lxml vulnerability (USN-4896-1)

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-4896-1 advisory.

It was discovered that lxml incorrectly handled certain HTML attributes. A remote attacker could possibly use this issue to perform cross-site scripting (XSS) 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-4896-1>

Solution

Update the affected python-lxml and / or python3-lxml 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

5.5 (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-2021-28957
XREF	USN:4896-1

Plugin Information

Published: 2021/03/30, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : python3-lxml_3.5.0-1ubuntu0.1
- Fixed package : python3-lxml_3.5.0-1ubuntu0.4

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_0.23.2-5~ubuntu16.04.1
- Fixed package : libp11-kit0_0.23.2-5~ubuntu16.04.2
- Installed package : p11-kit_0.23.2-5~ubuntu16.04.1
- Fixed package : p11-kit_0.23.2-5~ubuntu16.04.2
- Installed package : p11-kit-modules_0.23.2-5~ubuntu16.04.1
- Fixed package : p11-kit-modules_0.23.2-5~ubuntu16.04.2

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/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: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_1.2.3-1ubuntu0.2
- Fixed package : python3-cryptography_1.2.3-1ubuntu0.3

138552 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : snapd vulnerabilities (USN-4424-1)

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-4424-1 advisory.

It was discovered that cloud-init as managed by snapd on Ubuntu Core 16 and Ubuntu Core 18 devices ran on every boot without restrictions. A physical attacker could exploit this to craft cloud-init user- data/meta-data via external media to perform arbitrary changes on the device to bypass intended security mechanisms such as full disk encryption. This issue did not affect traditional Ubuntu systems.

(CVE-2020-11933)

It was discovered that snapctl user-open allowed altering the XDG_DATA_DIRS

environment variable when calling the system xdg-open. A malicious snap

could exploit this to bypass intended access restrictions to control how the host system xdg-open script opens the URL. This issue did not affect

Ubuntu Core systems. (CVE-2020-11934)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4424-1>

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

5.9 (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-2020-11933
CVE	CVE-2020-11934
XREF	USN:4424-1

Plugin Information

Published: 2020/07/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.45.1ubuntu0.2
- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.45.1ubuntu0.2

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
XREF
CVE-2020-27352
USN:4728-1

Plugin Information

Published: 2021/02/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.48.3

- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.48.3

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/V/C:H/I: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

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_1.28-2.1ubuntu0.1
- Fixed package : tar_1.28-2.1ubuntu0.2

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:OF/RC:C)

References

CVE	CVE-2020-26137
XREF	USN:4570-1

Plugin Information

Published: 2020/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.13.1-2ubuntu0.16.04.2
- Fixed package : python3-urllib3_1.13.1-2ubuntu0.16.04.4

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_2.4-0ubuntu6.3
- Fixed package : wpasupplicant_2.4-0ubuntu6.8

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 (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-2020-27748
XREF	USN:4649-1

Plugin Information

Published: 2020/11/26, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : xdg-utils_1.1.1-1ubuntu1.16.04.3
- Fixed package : xdg-utils_1.1.1-1ubuntu1.16.04.4
```

130586 - Ubuntu 16.04 LTS / 18.04 LTS : Apport regression (USN-4171-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4171-3 advisory.

USN-4171-1 fixed vulnerabilities in Apport. The update caused a regression in the Python Apport library.
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-4171-3>

Solution

Update the affected packages.

Risk Factor

Medium

References

XREF USN:4171-3

Plugin Information

Published: 2019/11/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.21
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.21
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.21
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.21

134657 - Ubuntu 16.04 LTS / 18.04 LTS : Apport regression (USN-4171-5)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4171-5 advisory.

USN-4171-1 fixed vulnerabilities in Apport. This caused a regression in autopkgtest and python2 compatibility.

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-4171-5>

Solution

Update the affected packages.

Risk Factor

Medium

References

XREF USN:4171-5

Plugin Information

Published: 2020/03/18, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.22
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.22
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.22
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.22

130396 - Ubuntu 16.04 LTS / 18.04 LTS : Apport vulnerabilities (USN-4171-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4171-1 advisory.

Kevin Backhouse discovered Apport would read its user-controlled settings file as the root user. This could be used by a local attacker to possibly crash Apport or have other unspecified consequences.

(CVE-2019-11481)

Sander Bos discovered a race-condition in Apport during core dump creation. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.

(CVE-2019-11482)

Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user. (CVE-2019-11483)

Sander Bos discovered Apport mishandled lock-file creation. This could be used by a local attacker to cause a denial of service against Apport. (CVE-2019-11485)

Kevin Backhouse discovered Apport read various process-specific files with elevated privileges during crash dump generation. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user. (CVE-2019-15790)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4171-1>

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

6.1 (CVSS2#AV:L/AC:L/Au:N/C:C/I:P/A:P)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-11481
CVE	CVE-2019-11482
CVE	CVE-2019-11483
CVE	CVE-2019-11485
CVE	CVE-2019-15790

Plugin Information

Published: 2019/10/30, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.20

- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.20

- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.20

- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.20
```

126567 - Ubuntu 16.04 LTS / 18.04 LTS : Apport vulnerability (USN-4051-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4051-1 advisory.

Kevin Backhouse discovered a race-condition when reading the user's local Apport configuration. This could be used by a local attacker to cause Apport to include arbitrary files in a resulting crash report.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4051-1>

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-2019-7307
XREF	USN:4051-1

Plugin Information

Published: 2019/07/09, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.19

- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.19

- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.19

- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.19
```

129967 - Ubuntu 16.04 LTS / 18.04 LTS : Aspell vulnerability (USN-4155-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4155-1 advisory.

It was discovered that Aspell incorrectly handled certain inputs. An attacker could potentially access 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-4155-1>

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-2019-17544
XREF	USN:4155-1

Plugin Information

Published: 2019/10/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : aspell_0.60.7~20110707-3build1
- Fixed package : aspell_0.60.7~20110707-3ubuntu0.1

- Installed package : libaspell15_0.60.7~20110707-3build1
- Fixed package : libaspell15_0.60.7~20110707-3ubuntu0.1
```

124323 - Ubuntu 16.04 LTS / 18.04 LTS : Bind vulnerability (USN-3956-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3956-1 advisory.

It was discovered that Bind incorrectly handled limiting the number of simultaneous TCP clients. A remote attacker could possibly use this issue to cause Bind 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-3956-1>

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

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-2018-5743
XREF	USN:3956-1

Plugin Information

Published: 2019/04/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : bind9-host_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : dnsutils_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libbind9-140_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns-export162_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libdns162_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc-export160_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisc160_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccc140_1:9.10.3.dfsg.P4-8ubuntu1.14
- Installed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : libisccfg140_1:9.10.3.dfsg.P4-8ubuntu1.14

- Installed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.12
- Fixed package : liblwres141_1:9.10.3.dfsg.P4-8ubuntu1.14

135027 - Ubuntu 16.04 LTS / 18.04 LTS : BlueZ vulnerabilities (USN-4311-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4311-1 advisory.

It was discovered that BlueZ incorrectly handled bonding HID and HOGP devices. A local attacker could possibly use this issue to impersonate non-bonded devices. (CVE-2020-0556)

It was discovered that BlueZ incorrectly handled certain commands. 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 16.04 LTS. (CVE-2016-7837)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4311-1>

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

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-2016-7837
CVE	CVE-2020-0556
XREF	USN:4311-1

Plugin Information

Published: 2020/03/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3
- Installed package : bluez-cups_5.37-0ubuntu5.1
- Fixed package : bluez-cups_5.37-0ubuntu5.3
- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3
- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3

128031 - Ubuntu 16.04 LTS / 18.04 LTS : CUPS vulnerabilities (USN-4105-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4105-1 advisory.

StephanZeisbergdiscovered that the CUPS SNMP backend incorrectly handled encoded ASN.1 inputs. A remote attacker could possibly use this issue to cause CUPS to crash by providing specially crafted network traffic. (CVE-2019-8696, CVE-2019-8675)

It was discovered that CUPS did not properly handle client disconnection events. A local attacker could possibly use this issue to cause a denial of service or disclose memory from the CUPS server.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4105-1>

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-2019-8675
CVE	CVE-2019-8696
XREF	USN:4105-1

Plugin Information

Published: 2019/08/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.10
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.10
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.10
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.10
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.10
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.10
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.10
- Installed package : cups-server-common_2.1.3-4ubuntu0.7

- Fixed package : cups-server-common_2.1.3-4ubuntu0.10
- Installed package : libcurl2_2.1.3-4ubuntu0.7
- Fixed package : libcurl2_2.1.3-4ubuntu0.10
- Installed package : libcurlcgi1_2.1.3-4ubuntu0.7
- Fixed package : libcurlcgi1_2.1.3-4ubuntu0.10
- Installed package : libcurlimage2_2.1.3-4ubuntu0.7
- Fixed package : libcurlimage2_2.1.3-4ubuntu0.10
- Installed package : libcurlsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcurlsmime1_2.1.3-4ubuntu0.10
- Installed package : libcurlspdc1_2.1.3-4ubuntu0.7
- Fixed package : libcurlspdc1_2.1.3-4ubuntu0.10

133352 - Ubuntu 16.04 LTS / 18.04 LTS : Cyrus SASL vulnerability (USN-4256-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4256-1 advisory.

It was discovered that Cyrus SASL incorrectly handled certain LDAP packets. An attacker could possibly use this issue to 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-4256-1>

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-2019-19906
XREF	USN:4256-1

Plugin Information

Published: 2020/01/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsasl2-2_2.1.26.dfsg1-14ubuntu0.1
- Fixed package : libsasl2-2_2.1.26.dfsg1-14ubuntu0.2
- Installed package : libsasl2-modules_2.1.26.dfsg1-14ubuntu0.1
- Fixed package : libsasl2-modules_2.1.26.dfsg1-14ubuntu0.2

- Installed package : `libsas12-modules-db_2.1.26.dfsg1-14ubuntu0.1`
- Fixed package : `libsas12-modules-db_2.1.26.dfsg1-14ubuntu0.2`

131226 - Ubuntu 16.04 LTS / 18.04 LTS : DjVuLibre vulnerabilities (USN-4198-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4198-1 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-4198-1>

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-2019-15142
CVE	CVE-2019-15143
CVE	CVE-2019-15144
CVE	CVE-2019-15145
CVE	CVE-2019-18804
XREF	USN:4198-1

Plugin Information

Published: 2019/11/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `libdjvulibre-text_3.5.27.1-5`
- Fixed package : `libdjvulibre-text_3.5.27.1-5ubuntu0.1`
- Installed package : `libdjvulibre21_3.5.27.1-5`
- Fixed package : `libdjvulibre21_3.5.27.1-5ubuntu0.1`

183631 - Ubuntu 16.04 LTS / 18.04 LTS : Evince vulnerability (USN-3959-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3959-1 advisory.

It was discovered that Evince incorrectly handled certain images. 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-3959-1>

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: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

4.3 (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-2019-11459
XREF	USN:3959-1

Plugin Information

Published: 2023/10/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : evince_3.18.2-1ubuntu4.3
- Fixed package : evince_3.18.2-1ubuntu4.4
- Installed package : evince-common_3.18.2-1ubuntu4.3
- Fixed package : evince-common_3.18.2-1ubuntu4.4
- Installed package : libevdocument3-4_3.18.2-1ubuntu4.3
- Fixed package : libevdocument3-4_3.18.2-1ubuntu4.4
- Installed package : libevview3-3_3.18.2-1ubuntu4.3
- Fixed package : libevview3-3_3.18.2-1ubuntu4.4

125621 - Ubuntu 16.04 LTS / 18.04 LTS : Evolution Data Server vulnerability (USN-3998-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3998-1 advisory.

Marcus Brinkmann discovered that Evolution Data Server did not correctly interpret the output from GPG when decrypting encrypted messages. Under certain circumstances, this could result in displaying clear- text portions of encrypted messages as though they were encrypted.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3998-1>

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

5.9 (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:P/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE-2018-15587
XREF USN:3998-1

Plugin Information

Published: 2019/05/31, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : evolution-data-server_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server_3.18.5-1ubuntu1.2
- Installed package : evolution-data-server-common_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server-common_3.18.5-1ubuntu1.2
- Installed package : evolution-data-server-online-accounts_3.18.5-1ubuntu1.1
- Fixed package : evolution-data-server-online-accounts_3.18.5-1ubuntu1.2
- Installed package : libcamel-1.2-54_3.18.5-1ubuntu1.1
- Fixed package : libcamel-1.2-54_3.18.5-1ubuntu1.2
- Installed package : libebackend-1.2-10_3.18.5-1ubuntu1.1
- Fixed package : libebackend-1.2-10_3.18.5-1ubuntu1.2
- Installed package : libebook-1.2-16_3.18.5-1ubuntu1.1
- Fixed package : libebook-1.2-16_3.18.5-1ubuntu1.2
- Installed package : libebook-contacts-1.2-2_3.18.5-1ubuntu1.1
- Fixed package : libebook-contacts-1.2-2_3.18.5-1ubuntu1.2
- Installed package : libecal-1.2-19_3.18.5-1ubuntu1.1
- Fixed package : libecal-1.2-19_3.18.5-1ubuntu1.2
- Installed package : libedata-book-1.2-25_3.18.5-1ubuntu1.1
- Fixed package : libedata-book-1.2-25_3.18.5-1ubuntu1.2
- Installed package : libedata-cal-1.2-28_3.18.5-1ubuntu1.1
- Fixed package : libedata-cal-1.2-28_3.18.5-1ubuntu1.2
- Installed package : libedataserver-1.2-21_3.18.5-1ubuntu1.1
- Fixed package : libedataserver-1.2-21_3.18.5-1ubuntu1.2
- Installed package : libedataserverui-1.2-1_3.18.5-1ubuntu1.1
- Fixed package : libedataserverui-1.2-1_3.18.5-1ubuntu1.2

126746 - Ubuntu 16.04 LTS / 18.04 LTS : Exiv2 vulnerabilities (USN-4056-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4056-1 advisory.

It was discovered that Exiv2 incorrectly handled certain PSD files. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-19107, CVE-2018-19108)

It was discovered that Exiv2 incorrectly handled certain PNG files. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-19535, CVE-2019-13112)

It was discovered that Exiv2 incorrectly handled certain CRW files. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-13110, CVE-2019-13113)

It was discovered that incorrectly handled certain HTTP requests. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-13114)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4056-1>

Solution

Update the affected exiv2, libexiv2-14 and / or libexiv2-dev 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-2018-19107
CVE	CVE-2018-19108
CVE	CVE-2018-19535
CVE	CVE-2019-13110
CVE	CVE-2019-13112
CVE	CVE-2019-13113
CVE	CVE-2019-13114
XREF	USN:4056-1

Plugin Information

Published: 2019/07/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexiv2-14_0.25-2.1ubuntu16.04.3
- Fixed package : libexiv2-14_0.25-2.1ubuntu16.04.4

[130148 - Ubuntu 16.04 LTS / 18.04 LTS : Exiv2 vulnerability \(USN-4159-1\)](#)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4159-1 advisory.

It was discovered that Exiv2 incorrectly handled certain 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-4159-1>

Solution

Update the affected exiv2, libexiv2-14 and / or libexiv2-dev 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:O/RC:C)

References

CVE
XREF
CVE-2019-17402
USN:4159-1

Plugin Information

Published: 2019/10/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexiv2-14_0.25-2.1ubuntu16.04.3
- Fixed package : libexiv2-14_0.25-2.1ubuntu16.04.5

128874 - Ubuntu 16.04 LTS / 18.04 LTS : Expat vulnerability (USN-4132-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4132-1 advisory.

It was discovered that Expat incorrectly handled certain XML 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-4132-1>

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
XREF

CVE-2019-15903
USN:4132-1

Plugin Information

Published: 2019/09/16, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libexpat1_2.1.0-7ubuntu0.16.04.3
- Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5

130200 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4165-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4165-1 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, bypass same-origin restrictions, conduct cross-site scripting (XSS) attacks, bypass content security policy (CSP) protections, 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-4165-1>

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-2018-6156
CVE	CVE-2019-11757
CVE	CVE-2019-11759
CVE	CVE-2019-11760
CVE	CVE-2019-11761
CVE	CVE-2019-11762
CVE	CVE-2019-11763
CVE	CVE-2019-11764
CVE	CVE-2019-11765
CVE	CVE-2019-15903
CVE	CVE-2019-17000
CVE	CVE-2019-17001
CVE XREF	CVE-2019-17002 USN:4165-1
XREF	IAVA:2019-A-0395-S

Plugin Information

Published: 2019/10/24, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_70.0+build2-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_70.0+build2-0ubuntu0.16.04.1

132854 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4234-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4234-1 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 Content Security Policy (CSP) restrictions, conduct cross-site scripting (XSS) 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-4234-1>

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

8.4 (CVSS:3.0/E:H/R:L/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

5.9 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2019-17016
CVE	CVE-2019-17017
CVE	CVE-2019-17020
CVE	CVE-2019-17022
CVE	CVE-2019-17023
CVE	CVE-2019-17024
CVE	CVE-2019-17025
CVE	CVE-2019-17026
XREF	USN:4234-1
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2020-0007

Plugin Information

Published: 2020/01/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_72.0.1+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_72.0.1+build1-0ubuntu0.16.04.1

135229 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-4317-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4317-1 advisory.

Two use-after-free bugs were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4317-1>

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

7.5 (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

II

References

CVE	CVE-2020-6819
CVE	CVE-2020-6820
XREF	USN:4317-1
XREF	IAVA:2020-A-0128-S
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2020-0032

Plugin Information

Published: 2020/04/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_74.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_74.0.1+build1-0ubuntu0.16.04.1

128026 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4101-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4101-1 advisory.

It was discovered that passwords could be copied to the clipboard from the Saved Logins dialog without entering the master password, even when a master password has been set. A local attacker could potentially exploit this to obtain saved 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-4101-1>

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

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-2019-11733
XREF USN:4101-1

Plugin Information

Published: 2019/08/20, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_68.0.2+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_68.0.2+build1-0ubuntu0.16.04.1

129385 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4140-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4140-1 advisory.

It was discovered that no user notification was given when pointer lock is enabled. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to hijack the mouse pointer and confuse users.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4140-1>

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:L/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.3 (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)

References

CVE-2019-11754
USN:4140-1

Plugin Information

Published: 2019/09/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_69.0.1+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_69.0.1+build1-0ubuntu0.16.04.1

183650 - Ubuntu 16.04 LTS / 18.04 LTS : GD Graphics Library vulnerabilities (USN-4316-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4316-1 advisory.

It was discovered that GD Graphics Library incorrectly handled cloning an image. An attacker could possibly use this issue to cause GD Graphics Library to crash, resulting in a denial of service.

(CVE-2018-14553)

It was discovered that GD Graphics Library incorrectly handled loading images from X bitmap format files.

An attacker could possibly use this issue to cause GD Graphics Library to crash, resulting in a denial of service, or to disclose contents of the stack that has been left there by previous code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2019-11038)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4316-1>

Solution

Update the affected libgd-dev, libgd-tools and / or libgd3 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-2018-14553
XREF	USN:4316-1

Plugin Information

Published: 2023/10/21, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libgd3_2.1.1-4ubuntu0.16.04.10
- Fixed package : libgd3_2.1.1-4ubuntu0.16.04.12

126565 - Ubuntu 16.04 LTS / 18.04 LTS : GLib vulnerability (USN-4049-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4049-1 advisory.

It was discovered that GLib created directories and files without properly restricting permissions. An attacker could possibly use this issue to access 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-4049-1>

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-2019-13012
XREF	USN:4049-1

Plugin Information

Published: 2019/07/09, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libglib2.0-0_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-0_2.48.2-0ubuntu4.3
- Installed package : libglib2.0-bin_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-bin_2.48.2-0ubuntu4.3
- Installed package : libglib2.0-data_2.48.2-0ubuntu4.1
- Fixed package : libglib2.0-data_2.48.2-0ubuntu4.3

130622 - Ubuntu 16.04 LTS / 18.04 LTS : GNU cpio vulnerability (USN-4176-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4176-1 advisory.

Thomas Habets discovered that GNU cpio incorrectly handled certain inputs. An attacker could possibly use this issue to 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-4176-1>

Solution

Update the affected cpio and / or cpio-win32 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

6.6 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-14866
XREF	USN:4176-1

Plugin Information

Published: 2019/11/07, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : cpio_2.11+dfsg-5ubuntu1
- Fixed package : cpio_2.11+dfsg-5ubuntu1.1
```

124408 - Ubuntu 16.04 LTS / 18.04 LTS : GStreamer Base Plugins vulnerability (USN-3958-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3958-1 advisory.

It was discovered that GStreamer Base Plugins did not correctly handle certain malformed RTSP streams. If a user were tricked into opening a crafted RTSP stream with a GStreamer application, an attacker could cause a denial of service via 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-3958-1>

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-2019-9928

XREF USN:3958-1

Plugin Information

Published: 2019/04/30, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-gst-plugins-base-1.0_1.8.3-1ubuntu0.2
- Fixed package : gir1.2-gst-plugins-base-1.0_1.8.3-1ubuntu0.3

- Installed package : gstreamer1.0-alsa_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-alsa_1.8.3-1ubuntu0.3

- Installed package : gstreamer1.0-plugins-base_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-plugins-base_1.8.3-1ubuntu0.3

- Installed package : gstreamer1.0-plugins-base-apps_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-plugins-base-apps_1.8.3-1ubuntu0.3

- Installed package : gstreamer1.0-x_1.8.3-1ubuntu0.2
- Fixed package : gstreamer1.0-x_1.8.3-1ubuntu0.3

- Installed package : libgstreamer-plugins-base1.0-0_1.8.3-1ubuntu0.2
- Fixed package : libgstreamer-plugins-base1.0-0_1.8.3-1ubuntu0.3
```

126598 - Ubuntu 16.04 LTS / 18.04 LTS : GVfs vulnerabilities (USN-4053-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4053-1 advisory.

It was discovered that GVfs incorrectly handled the admin backend. Files created or moved by the admin backend could end up with the wrong ownership information, contrary to expectations. This issue only affected Ubuntu 18.04 LTS, Ubuntu 18.10, and Ubuntu 19.04. (CVE-2019-12447, CVE-2019-12448, CVE-2019-12449)

It was discovered that GVfs incorrectly handled authentication on its private D-Bus socket. A local attacker could possibly connect to this socket and issue D-Bus calls. (CVE-2019-12795)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4053-1>

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-2019-12447
CVE	CVE-2019-12448
CVE	CVE-2019-12449
CVE	CVE-2019-12795
XREF	USN:4053-1

Plugin Information

Published: 2019/07/10, Modified: 2025/02/25

Plugin Output

tcp/0

- Installed package : gvfs_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-backends_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-backends_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-bin_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-bin_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-common_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-common_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-daemons_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-daemons_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-fuse_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-fuse_1.28.2-1ubuntu1~16.04.3
- Installed package : gvfs-libs_1.28.2-1ubuntu1~16.04.2
- Fixed package : gvfs-libs_1.28.2-1ubuntu1~16.04.3

144787 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-4686-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4686-1 advisory.

It was discovered that Ghostscript incorrectly handled certain image 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-4686-1>

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-2018-5727
CVE	CVE-2020-6851
CVE	CVE-2020-8112
CVE	CVE-2020-27814
CVE	CVE-2020-27824
CVE	CVE-2020-27841
CVE	CVE-2020-27842
CVE	CVE-2020-27843
CVE	CVE-2020-27845
XREF	USN:4686-1
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/01/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.14
- Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.14
- Installed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.14
- Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.14

124717 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerability (USN-3970-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3970-1 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-3970-1>

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-2019-3839
XREF	USN:3970-1

Plugin Information

Published: 2019/05/09, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0-0ubuntu0.16.04.9
- Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.16.04.9
- Installed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0-0ubuntu0.16.04.9
- Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0-0ubuntu0.16.04.9

127840 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerability (USN-4092-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4092-1 advisory.

Netanel Fisher discovered that the font handler in Ghostscript did not properly restrict privileged calls when '-dSAFER' restrictions were in effect. 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4092-1>

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)

STIG Severity

I

References

CVE	CVE-2019-10216
XREF	USN:4092-1
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/08/13, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript_9.26~dfsg+0~0ubuntu0.16.04.10
- Installed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.10
- Installed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9_9.26~dfsg+0~0ubuntu0.16.04.10
- Installed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7
- Fixed package : libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.10

131073 - Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerability (USN-4193-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4193-1 advisory.

Paul Manfred and Lukas Schauer 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-4193-1>

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-2019-14869
XREF	USN:4193-1
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/11/15, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.12`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.12`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.12`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.12`

125622 - Ubuntu 16.04 LTS / 18.04 LTS : GnuTLS vulnerabilities (USN-3999-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3999-1 advisory.

Eyal Ronen, Kenneth G. Paterson, and Adi Shamir discovered that GnuTLS was vulnerable to a timing side-channel attack known as the Lucky Thirteen issue. A remote attacker could possibly use this issue to perform plaintext-recovery attacks via analysis of timing data. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-10844, CVE-2018-10845, CVE-2018-10846)

Tavis Ormandy discovered that GnuTLS incorrectly handled memory when verifying certain X.509 certificates.

A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 18.10, and Ubuntu 19.04. (CVE-2019-3829)

It was discovered that GnuTLS incorrectly handled certain post-handshake messages. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.10 and Ubuntu 19.04. (CVE-2019-3836)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3999-1>

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

5.3 (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-2018-10844
CVE	CVE-2018-10845
CVE	CVE-2018-10846
CVE	CVE-2019-3829
CVE	CVE-2019-3836
XREF	USN:3999-1

Plugin Information

Published: 2019/05/31, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libgnutls-openssl27_3.4.10-4ubuntu1.4
- Fixed package : libgnutls-openssl27_3.4.10-4ubuntu1.5

- Installed package : libgnutls30_3.4.10-4ubuntu1.4
- Fixed package : libgnutls30_3.4.10-4ubuntu1.5
```

134663 - Ubuntu 16.04 LTS / 18.04 LTS : ICU vulnerability (USN-4305-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4305-1 advisory.

Andr Bargull discovered that ICU incorrectly handled certain strings. 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-4305-1>

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-2020-10531
XREF	USN:4305-1

Plugin Information

Published: 2020/03/18, Modified: 2024/08/27

Plugin Output

- Installed package : libicu55_55.1-7ubuntu0.4
- Fixed package : libicu55_55.1-7ubuntu0.5

126254 - Ubuntu 16.04 LTS / 18.04 LTS : ImageMagick vulnerabilities (USN-4034-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4034-1 advisory.

It was discovered that ImageMagick incorrectly handled certain malformed image files. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or possibly execute code with the privileges of the user invoking the program.

Due to a large number of issues discovered in GhostScript that prevent it from being used by ImageMagick safely, the update for Ubuntu 18.10 and Ubuntu 19.04 includes a default policy change that disables support for the Postscript and PDF formats in ImageMagick. This policy can be overridden if necessary by using an alternate ImageMagick policy configuration.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4034-1>

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-2017-12805
CVE	CVE-2017-12806
CVE	CVE-2018-14434
CVE	CVE-2018-15607
CVE	CVE-2018-16323
CVE	CVE-2018-16412
CVE	CVE-2018-16413
CVE	CVE-2018-16644
CVE	CVE-2018-16645
CVE	CVE-2018-17965
CVE	CVE-2018-17966
CVE	CVE-2018-18016
CVE	CVE-2018-18023
CVE	CVE-2018-18024
CVE	CVE-2018-18025
CVE	CVE-2018-18544
CVE	CVE-2018-20467
CVE	CVE-2019-10131
CVE	CVE-2019-10649
CVE	CVE-2019-10650

CVE	CVE-2019-11470
CVE	CVE-2019-11472
CVE	CVE-2019-11597
CVE	CVE-2019-11598
CVE	CVE-2019-7175
CVE	CVE-2019-7395
CVE	CVE-2019-7396
CVE	CVE-2019-7397
CVE	CVE-2019-7398
XREF	CVE-2019-9956 USN:4034-1

Plugin Information

Published: 2019/06/26, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.14

- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.14

- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.14

- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.14

- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.14

- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.14
```

131072 - Ubuntu 16.04 LTS / 18.04 LTS : ImageMagick vulnerabilities (USN-4192-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4192-1 advisory.

It was discovered that ImageMagick incorrectly handled certain malformed image files. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service or possibly execute code with the privileges of the user invoking the program.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4192-1>

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-2019-12974
CVE	CVE-2019-12975
CVE	CVE-2019-12976
CVE	CVE-2019-12977
CVE	CVE-2019-12978
CVE	CVE-2019-12979
CVE	CVE-2019-13135
CVE	CVE-2019-13137
CVE	CVE-2019-13295
CVE	CVE-2019-13297
CVE	CVE-2019-13300
CVE	CVE-2019-13301
CVE	CVE-2019-13304
CVE	CVE-2019-13305
CVE	CVE-2019-13306
CVE	CVE-2019-13307
CVE	CVE-2019-13308
CVE	CVE-2019-13309
CVE	CVE-2019-13310
CVE	CVE-2019-13311
CVE	CVE-2019-13391
CVE	CVE-2019-13454
CVE	CVE-2019-14981
CVE	CVE-2019-15139
CVE	CVE-2019-15140
CVE	CVE-2019-16708
CVE	CVE-2019-16709
CVE	CVE-2019-16710
CVE	CVE-2019-16711
CVE	CVE-2019-16713
XREF	USN:4192-1
XREF	IAVB:2019-B-0062-S

Plugin Information

Published: 2019/11/15, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : imagemagick_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick_8:6.8.9.9-7ubuntu5.15
- Installed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-6.q16_8:6.8.9.9-7ubuntu5.15
- Installed package : imagemagick-common_8:6.8.9.9-7ubuntu5.13
- Fixed package : imagemagick-common_8:6.8.9.9-7ubuntu5.15
- Installed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2_8:6.8.9.9-7ubuntu5.15
- Installed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickcore-6.q16-2-extra_8:6.8.9.9-7ubuntu5.15
- Installed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.13
- Fixed package : libmagickwand-6.q16-2_8:6.8.9.9-7ubuntu5.15

125353 - Ubuntu 16.04 LTS / 18.04 LTS : Intel Microcode update (USN-3977-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3977-2 advisory.

USN-3977-1 provided mitigations for Microarchitectural Data Sampling (MDS) vulnerabilities in Intel Microcode for a large number of Intel processor families. This update provides the corresponding updated microcode mitigations for Intel Cherry Trail and Bay Trail processor families.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3977-2>

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

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

5.1 (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-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2019-11091
XREF	USN:3977-2
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/05/23, Modified: 2025/02/27

Plugin Output

tcp/0

- Installed package : intel-microcode 3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20190514.0ubuntu0.16.04.2

125771 - Ubuntu 16.04 LTS / 18.04 LTS : Jinja2 vulnerabilities (USN-4011-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4011-1 advisory.

Olivier Dony discovered that Jinja incorrectly handled str.format. An attacker could possibly use this issue to escape the sandbox. This issue only affected Ubuntu 16.04 LTS. (CVE-2016-10745)

Brian Welch discovered that Jinja incorrectly handled str.format_map. An attacker could possibly use this issue to escape the sandbox. (CVE-2019-10906)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4011-1>

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

7.5 (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)

References

CVE	CVE-2016-10745
XREF	USN:4011-1

Plugin Information

Published: 2019/06/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-jinja2 2.8-1
- Fixed package : python3-jinja2 2.8-1ubuntu0.1

125337 - Ubuntu 16.04 LTS / 18.04 LTS : LibRaw vulnerabilities (USN-3989-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3989-1 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-3989-1>

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-2018-20337
CVE	CVE-2018-20363
CVE	CVE-2018-20364
CVE	CVE-2018-20365
CVE	CVE-2018-5817
CVE	CVE-2018-5818
CVE	CVE-2018-5819
XREF	USN:3989-1

Plugin Information

Published: 2019/05/22, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libraw15_0.17.1-1ubuntu0.4
- Fixed package : libraw15_0.17.1-1ubuntu0.5
```

130052 - Ubuntu 16.04 LTS / 18.04 LTS : LibTIFF vulnerabilities (USN-4158-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4158-1 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-4158-1>

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-2019-14973
CVE	CVE-2019-17546
XREF	USN:4158-1

Plugin Information

Published: 2019/10/18, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libtiff5_4.0.6-1ubuntu0.5
- Fixed package : libtiff5_4.0.6-1ubuntu0.7

129351 - Ubuntu 16.04 LTS / 18.04 LTS : LibreOffice vulnerability (USN-4138-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4138-1 advisory.

It was discovered that LibreOffice incorrectly handled embedded scripts in document files. If a user were tricked into opening a specially crafted document, a remote attacker could 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-4138-1>

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)

STIG Severity

II

References

CVE	CVE-2019-9854
XREF	USN:4138-1
XREF	IAVB:2019-B-0078-S

Plugin Information

Published: 2019/09/25, Modified: 2024/08/27

Plugin Output

tcp/0

```

- Installed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial6
- Fixed package : fonts-opensymbol_2:102.7+Lib05.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-avmedia-backend-gstreamer_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-base-core_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-calc_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-common_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-core_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-draw_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gnome_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-gtk_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-impress_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-math_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-ogltrans_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-pdfimport_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-breeze_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-style-galaxy_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : libreoffice-writer_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : python3-uno_1:5.1.6~rc2-0ubuntu1~xenial10

- Installed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : uno-libs3_5.1.6~rc2-0ubuntu1~xenial10

- Installed package : ure_5.1.6~rc2-0ubuntu1~xenial6
- Fixed package : ure_5.1.6~rc2-0ubuntu1~xenial10

```

130167 - Ubuntu 16.04 LTS / 18.04 LTS : Libxslt vulnerabilities (USN-4164-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4164-1 advisory.

It was discovered that Libxslt incorrectly handled certain documents. An attacker could possibly use this issue to access sensitive information. This issue not affected Ubuntu 19.10. (CVE-2019-13117, CVE-2019-13118)

It was discovered that Libxslt incorrectly handled certain documents. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-18197)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4164-1>

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 (CVSS:2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS:2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-13117
CVE	CVE-2019-13118
CVE	CVE-2019-18197
XREF	USN:4164-1

Plugin Information

Published: 2019/10/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libxslt1.1_1.1.28-2.1ubuntu0.1
- Fixed package : libxslt1.1_1.1.28-2.1ubuntu0.3

136400 - Ubuntu 16.04 LTS / 18.04 LTS : Linux firmware vulnerability (USN-4351-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4351-1 advisory.

Eli Biham and Lior Neumann discovered that certain Bluetooth devices incorrectly validated key exchange parameters. An 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-4351-1>

Solution

Update the affected linux-firmware, nic-firmware and / or scsi-firmware packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:A/AC:H/PR:N/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

4.3 (CVSS:2#AV:A/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

References

CVE	CVE-2018-5383
XREF	USN:4351-1

Plugin Information

Published: 2020/05/07, Modified: 2025/02/21

Plugin Output

tcp/0

- Installed package : linux-firmware_1.157.21
- Fixed package : linux-firmware_1.157.23

126374 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel update (USN-4041-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4041-1 advisory.

USN-4017-1 fixed vulnerabilities in the Linux kernel for Ubuntu. Unfortunately, the update introduced a regression that interfered with networking applications that setup very low SO_SNDBUF values. This update fixes the problem.

We apologize for the inconvenience.

Jonathan Looney discovered that the Linux kernel could be coerced into segmenting responses into multiple TCP segments. A remote attacker could construct an ongoing sequence of requests 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-4041-1>

Solution

Update the affected kernel 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-2019-11479
XREF	USN:4041-1
XREF	CEA-ID:CEA-2019-0456

Plugin Information

Published: 2019/07/01, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-54-generic for this advisory.

129490 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4144-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4144-1 advisory.

It was discovered that the XFS file system in the Linux kernel did not properly handle mount failures in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2018-20976)

Benjamin Moody discovered that the XFS file system in the Linux kernel did not properly handle an error condition when out of disk quota. A local attacker could possibly use this to cause a denial of service.
(CVE-2019-15538)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4144-1>

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-2018-20976
CVE	CVE-2019-15538
XREF	USN:4144-1

Plugin Information

Published: 2019/10/01, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-65-generic for this advisory.

133800 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4287-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4287-1 advisory.

It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information. (CVE-2019-14615)

It was discovered that the Atheros 802.11ac wireless USB device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15099)

It was discovered that the HSA Linux kernel driver for AMD GPU devices did not properly check for errors in certain situations, leading to a NULL pointer dereference. A local attacker could possibly use this to cause a denial of service. (CVE-2019-16229)

It was discovered that the Marvell 8xxx Libertas WLAN device driver in the Linux kernel did not properly check for errors in certain situations, leading to a NULL pointer dereference. A local attacker could possibly use this to cause a denial of service. (CVE-2019-16232)

It was discovered that a race condition existed in the Virtual Video Test Driver in the Linux kernel. An attacker with write access to /dev/video0 on a system with the vivid module loaded could possibly use this to gain administrative privileges. (CVE-2019-18683)

It was discovered that the Renesas Digital Radio Interface (DRIF) driver in the Linux kernel did not properly initialize data. A local attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2019-18786)

It was discovered that the Afatech AF9005 DVB-T USB device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-18809)

It was discovered that the btrfs file system in the Linux kernel did not properly validate metadata, leading to a NULL pointer dereference. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service (system crash). (CVE-2019-18885)

It was discovered that multiple memory leaks existed in the Marvell WiFi-Ex Driver for the Linux kernel. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19057)

It was discovered that the crypto subsystem in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19062)

It was discovered that the Realtek rtlwifi USB device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19063)

It was discovered that the RSI 91x WLAN device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19071)

It was discovered that the Atheros 802.11ac wireless USB device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19078)

It was discovered that the AMD GPU device drivers in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to possibly cause a denial of service (kernel memory exhaustion). (CVE-2019-19082)

Dan Carpenter discovered that the AppleTalk networking subsystem of the Linux kernel did not properly handle certain error conditions, leading to a NULL pointer dereference. A local attacker could use this to cause a denial of service (system crash). (CVE-2019-19227)

It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly handle ioctl requests to get emulated CPUID features. An attacker with access to /dev/kvm could use this to cause a denial of service (system crash). (CVE-2019-19332)

It was discovered that the ext4 file system implementation in the Linux kernel did not properly handle certain conditions. An attacker could use this to specially craft an ext4 file system that, when mounted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-19767)

Gao Chuan discovered that the SAS Class driver in the Linux kernel contained a race condition that could lead to a NULL pointer dereference. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-19965)

It was discovered that the Datagram Congestion Control Protocol (DCCP) implementation in the Linux kernel did not properly deallocate memory in certain error conditions. An attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-20096)

Mitchell Frank discovered that the Wi-Fi implementation in the Linux kernel when used as an access point would send IAPP location updates for stations before client authentication had completed. A physically proximate attacker could use this to cause a denial of service. (CVE-2019-5108)

It was discovered that a race condition can lead to a use-after-free while destroying GEM contexts in the i915 driver for the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-7053)

It was discovered that the B2C2 FlexCop USB device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15291)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4287-1>

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:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-14615
CVE	CVE-2019-15099
CVE	CVE-2019-15291
CVE	CVE-2019-16229
CVE	CVE-2019-16232
CVE	CVE-2019-18683
CVE	CVE-2019-18786
CVE	CVE-2019-18809
CVE	CVE-2019-18885
CVE	CVE-2019-19057
CVE	CVE-2019-19062
CVE	CVE-2019-19063
CVE	CVE-2019-19071
CVE	CVE-2019-19078
CVE	CVE-2019-19082
CVE	CVE-2019-19227
CVE	CVE-2019-19332
CVE	CVE-2019-19767
CVE	CVE-2019-19965
CVE	CVE-2019-20096
CVE	CVE-2019-5108
CVE	CVE-2020-7053
XREF	USN:4287-1

Plugin Information

Published: 2020/02/19, Modified: 2024/08/29

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-88-generic for this advisory.

136088 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4345-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4345-1 advisory.

Al Viro discovered that the Linux kernel for s390x systems did not properly perform page table upgrades for kernel sections that use secondary address mode. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2020-11884)

It was discovered that the Intel Wi-Fi driver in the Linux kernel did not properly check for errors in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2019-16234)

Tristan Madani discovered that the block I/O tracing implementation in the Linux kernel contained a race condition. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2019-19768)

It was discovered that the vhost net driver in the Linux kernel contained a stack buffer overflow. A local attacker with the ability to perform ioctl() calls on /dev/vhost-net could use this to cause a denial of service (system crash). (CVE-2020-10942)

It was discovered that the OV51x USB Camera device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-11608)

It was discovered that the STV06XX USB Camera device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-11609)

It was discovered that the Xirlink C-It USB Camera device driver in the Linux kernel did not properly validate device metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-11668)

It was discovered that the virtual terminal implementation in the Linux kernel contained a race condition.

A local attacker could possibly use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2020-8648)

Jordy Zomer discovered that the floppy driver in the Linux kernel did not properly check for errors in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2020-9383)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4345-1>

Solution

Update the affected kernel package.

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

6.9 (CVSS:2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS:2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-16234
CVE	CVE-2019-19768
CVE	CVE-2020-10942
CVE	CVE-2020-11608
CVE	CVE-2020-11609
CVE	CVE-2020-11668
CVE	CVE-2020-11884
CVE	CVE-2020-8648
CVE	CVE-2020-9383
XREF	USN:4345-1

Plugin Information

Published: 2020/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-99-generic for this advisory.

136710 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4363-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4363-1 advisory.

It was discovered that the Serial CAN interface driver in the Linux kernel did not properly initialize data. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2020-11494)

It was discovered that the linux kernel did not properly validate certain mount options to the tmpfs virtual memory file system. A local attacker with the ability to specify mount options could use this to cause a denial of service (system crash). (CVE-2020-11565)

David Gibson discovered that the Linux kernel on Power9 CPUs did not properly save and restore Authority Mask registers state in some situations. A local attacker in a guest VM could use this to cause a denial of service (host system crash). (CVE-2020-11669)

It was discovered that the block layer 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-2020-12657)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4363-1>

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-2020-11494
CVE	CVE-2020-11565
CVE	CVE-2020-11669
CVE	CVE-2020-12657
XREF	USN:4363-1

Plugin Information

Published: 2020/05/19, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-101-generic for this advisory.

141448 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4578-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4578-1 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)

Wen Xu discovered that the XFS file system in the Linux kernel did not properly validate inode metadata in some situations. An attacker could use this to construct a malicious XFS image that, when mounted, could cause a denial of service (system crash). (CVE-2018-10322)

It was discovered that the btrfs file system in the Linux kernel contained a use-after-free vulnerability when merging free space. An attacker could use this to construct a malicious btrfs image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2019-19448)

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)

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 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)

It was discovered that the NFC implementation in the Linux kernel did not properly perform permissions checks when opening raw sockets. A local attacker could use this to create or listen to NFC traffic.
(CVE-2020-26088)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4578-1>

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

BID	103960
CVE	CVE-2018-10322
CVE	CVE-2019-19448
CVE	CVE-2020-14314
CVE	CVE-2020-16119
CVE	CVE-2020-16120
CVE	CVE-2020-25212
CVE	CVE-2020-26088
XREF	USN:4578-1

Plugin Information

Published: 2020/10/14, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-120-generic for this advisory.

147972 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4883-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4883-1 advisory.

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)

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-4883-1>

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-2021-27363
CVE	CVE-2021-27364
CVE	CVE-2021-27365
XREF	USN:4883-1

Plugin Information

Published: 2021/03/23, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-139-generic for this advisory.

190855 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6647-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6647-1 advisory.

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)

It was discovered that the netfilter connection tracker for netlink 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-2023-7192)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6647-1>

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-2023-7192
CVE	CVE-2023-51780
CVE	CVE-2023-51782
XREF	USN:6647-1

Plugin Information

Published: 2024/02/21, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-222-generic for this advisory.

197215 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6777-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6777-1 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:

- Block layer subsystem;
- Userspace I/O drivers;
- Ceph distributed file system;
- Ext4 file system;
- JFS file system;
- NILFS2 file system;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Logical Link layer;
- MAC80211 subsystem;
- Netlink;
- NFC subsystem;
- Tomoyo security module; (CVE-2023-52524, CVE-2023-52530, CVE-2023-52601, CVE-2023-52439, CVE-2024-26635, CVE-2023-52602, CVE-2024-26614, CVE-2024-26704, CVE-2023-52604, CVE-2023-52566, CVE-2021-46981, CVE-2024-26622, CVE-2024-26735, CVE-2024-26805, CVE-2024-26801, CVE-2023-52583)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6777-1>

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:O/RC:C)

References

CVE	CVE-2021-46981
CVE	CVE-2023-47233
CVE	CVE-2023-52439
CVE	CVE-2023-52524

CVE	CVE-2023-52530
CVE	CVE-2023-52566
CVE	CVE-2023-52583
CVE	CVE-2023-52601
CVE	CVE-2023-52602
CVE	CVE-2023-52604
CVE	CVE-2024-26614
CVE	CVE-2024-26622
CVE	CVE-2024-26635
CVE	CVE-2024-26704
CVE	CVE-2024-26735
CVE	CVE-2024-26801
XREF	CVE-2024-26805 USN:6777-1

Plugin Information

Published: 2024/05/16, Modified: 2025/01/15

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-225-generic for this advisory.

201860 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6866-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6866-1 advisory.

It was discovered that the ext4 file system implementation in the Linux kernel did not properly validate data state on write operations. 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-2021-33631)

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)

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)

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)

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)

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:

- Block layer subsystem;
- Hardware random number generator core;
- GPU drivers;
- AFS file system;
- Memory management;
- Netfilter; (CVE-2024-26642, CVE-2024-26922, CVE-2024-26720, CVE-2024-26736, CVE-2024-26898, CVE-2021-47063, CVE-2023-52615)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6866-1>

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-2021-33631
CVE	CVE-2021-47063
CVE	CVE-2023-6270
CVE	CVE-2023-52615
CVE	CVE-2024-2201
CVE	CVE-2024-23307
CVE	CVE-2024-24861
CVE	CVE-2024-26642
CVE	CVE-2024-26720
CVE	CVE-2024-26736
CVE	CVE-2024-26898
CVE	CVE-2024-26922
XREF	USN:6866-1

Plugin Information

Published: 2024/07/03, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-226-generic for this advisory.

204834 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6926-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6926-1 advisory.

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)

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)

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)

Supraja Sridhara, Benedict Schlter, Mark Kuhne, Andrin Bertschi, and Shweta Shinde discovered that the Confidential Computing framework in the Linux kernel for x86 platforms did not properly handle 32-bit emulation on TDX and SEV. An attacker with access to the VMM could use this to cause a denial of service (guest crash) or possibly execute arbitrary code. (CVE-2024-25744)

11/2/25, 1:18 AM

Photographer

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;
- HID subsystem;
- I2C subsystem;
- MTD block device drivers;
- Network drivers;
- TTY drivers;
- USB subsystem;
- File systems infrastructure;
- F2FS file system;
- SMB network file system;
- BPF subsystem;
- B.A.T.M.A.N. meshing protocol;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Netfilter;
- Unix domain sockets;
- AppArmor security module; (CVE-2023-52435, CVE-2024-27013, CVE-2024-35984, CVE-2023-52620, CVE-2024-35997, CVE-2023-52436, CVE-2024-26884, CVE-2024-26901, CVE-2023-52469, CVE-2024-35978, CVE-2024-26886, CVE-2024-35982, CVE-2024-36902, CVE-2024-26857, CVE-2024-26923, CVE-2023-52443, CVE-2024-27020, CVE-2024-36016, CVE-2024-26840, CVE-2024-26934, CVE-2023-52449, CVE-2024-26882, CVE-2023-52444, CVE-2023-52752)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6926-1>

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

7.7 (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-2023-46343
CVE	CVE-2023-52435
CVE	CVE-2023-52436
CVE	CVE-2023-52443
CVE	CVE-2023-52444
CVE	CVE-2023-52449
CVE	CVE-2023-52469
CVE	CVE-2023-52620
CVE	CVE-2023-52752
CVE	CVE-2024-24857
CVE	CVE-2024-24858
CVE	CVE-2024-24859
CVE	CVE-2024-25739
CVE	CVE-2024-25744
CVE	CVE-2024-26840
CVE	CVE-2024-26857
CVE	CVE-2024-26882
CVE	CVE-2024-26884
CVE	CVE-2024-26886
CVE	CVE-2024-26901
CVE	CVE-2024-26923
CVE	CVE-2024-26934
CVE	CVE-2024-27013
CVE	CVE-2024-27020
CVE	CVE-2024-35978
CVE	CVE-2024-35982
CVE	CVE-2024-35984
CVE	CVE-2024-35997
CVE	CVE-2024-36016
CVE	CVE-2024-36902
XREF	USN:6926-1

Plugin Information

Published: 2024/07/29, Modified: 2024/09/09

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-227-generic for this advisory.

206075 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6972-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6972-1 advisory.

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)

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;
- User-Mode Linux (UML);
- GPU drivers;
- MMC subsystem;
- Network drivers;
- PHY drivers;
- Pin controllers subsystem;

- Xen hypervisor drivers;
- GFS2 file system;
- Core kernel;
- Bluetooth subsystem;
- IPv4 networking;
- IPv6 networking;
- HD-audio driver;

- ALSA SH drivers; (CVE-2024-26903, CVE-2024-35835, CVE-2023-52644, CVE-2024-39292, CVE-2024-36940, CVE-2024-26600, CVE-2023-52629, CVE-2024-35955, CVE-2023-52760, CVE-2023-52806, CVE-2024-39484, CVE-2024-26679, CVE-2024-26654, CVE-2024-36901, CVE-2024-26687, CVE-2023-52470)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6972-1>

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:2.0/AV:L/AC:L/Au:S/C:I/C:A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS:2.0/E:U/RL:OF/RC:C)

References

CVE	CVE-2023-52470
CVE	CVE-2023-52629
CVE	CVE-2023-52644
CVE	CVE-2023-52760
CVE	CVE-2023-52806
CVE	CVE-2024-22099
CVE	CVE-2024-24860
CVE	CVE-2024-26600
CVE	CVE-2024-26654
CVE	CVE-2024-26679
CVE	CVE-2024-26687
CVE	CVE-2024-26903
CVE	CVE-2024-35835
CVE	CVE-2024-35955
CVE	CVE-2024-36901
CVE	CVE-2024-36940
CVE	CVE-2024-39292
CVE	CVE-2024-39484
XREF	USN:6972-1

Plugin Information

Published: 2024/08/21, Modified: 2025/01/13

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-228-generic for this advisory.

209060 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7069-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7069-1 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:

- x86 architecture;
 - Cryptographic API;
 - CPU frequency scaling framework;
 - HW tracing;
 - ISDN/mISDN subsystem;
 - Media drivers;
 - Network drivers;
 - NVME drivers;
 - S/390 drivers;
 - SCSI drivers;
 - USB subsystem;
 - VFIO drivers;
 - Watchdog drivers;
 - JFS file system;
 - IRQ subsystem;
 - Core kernel;
 - Memory management;
 - Amateur Radio drivers;
 - IPv4 networking;
 - IPv6 networking;
 - IUCV driver;
 - Network traffic control;
 - TIPC protocol;
 - XFRM subsystem;
 - Integrity Measurement Architecture
 - SoC Audio for Freescale CPUs driver

2024-31076, CVE-2024-26754, CVE-2023-52510, CVE-2024-40941, CVE-2024-45016, CVE-2024-38627, CVE-2024-38621, CVE-2024-39487, CVE-2024-27436, CVE-2024-40901, CVE-2024-26812, CVE-2024-42244, CVE-2024-42229, CVE-2024-43858, CVE-2024-42280, CVE-2024-26641, CVE-2024-42284, CVE-2024-26602

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7069-1>

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-2023-52510
CVE	CVE-2023-52528
CVE	CVE-2024-26602
CVE	CVE-2024-26641
CVE	CVE-2024-26754
CVE	CVE-2024-26810
CVE	CVE-2024-26812
CVE	CVE-2024-26960
CVE	CVE-2024-27051
CVE	CVE-2024-27436
CVE	CVE-2024-31076
CVE	CVE-2024-36971
CVE	CVE-2024-38602
CVE	CVE-2024-38611
CVE	CVE-2024-38621
CVE	CVE-2024-38627
CVE	CVE-2024-38630
CVE	CVE-2024-39487
CVE	CVE-2024-39494
CVE	CVE-2024-40901
CVE	CVE-2024-40941
CVE	CVE-2024-41073
CVE	CVE-2024-41097
CVE	CVE-2024-42089
CVE	CVE-2024-42157
CVE	CVE-2024-42223
CVE	CVE-2024-42229
CVE	CVE-2024-42244
CVE	CVE-2024-42271
CVE	CVE-2024-42280
CVE	CVE-2024-42284
CVE	CVE-2024-43858
CVE	CVE-2024-44940
CVE	CVE-2024-45016
CVE	CVE-2024-46673
XREF	CISA-KNOWN-EXPLOITED:2024/08/28
XREF	USN:7069-1

Plugin Information

Published: 2024/10/15, Modified: 2024/10/15

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-230-generic for this advisory.

211624 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7121-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7121-1 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;

- S390 architecture;

- x86 architecture;

- Block layer subsystem;

- Cryptographic API;

- ATM drivers;

- Device frequency scaling framework;

- GPU drivers;

- Hardware monitoring drivers;

- VMware VMCI Driver;

- Network drivers;

- Device tree and open firmware driver;

- SCSI drivers;

- Greybus lights staging drivers;

- BTRFS file system;

- File systems infrastructure;

- F2FS file system;

- JFS file system;

- NILFS2 file system;

- Netfilter;

- Memory management;

- Ethernet bridge;

- IPv6 networking;

- IUCV driver;

- Logical Link layer;

- MAC80211 subsystem;

- NFC subsystem;

- Network traffic control;

- Unix domain sockets; (CVE-2023-52614, CVE-2024-26633, CVE-2024-46758, CVE-2024-46723, CVE-2023-52502, CVE-2024-41059, CVE-2024-44987, CVE-2024-36020, CVE-2023-52599, CVE-2023-52639, CVE-2024-26668, CVE-2024-42094, CVE-2022-48938, CVE-2022-48733, CVE-2024-27397, CVE-2023-52578, CVE-2024-38560, CVE-2024-38538, CVE-2024-42310, CVE-2024-46722, CVE-2024-46800, CVE-2024-41095, CVE-2024-42104, CVE-2024-35877, CVE-2022-48943, CVE-2024-46743, CVE-2023-52531, CVE-2024-46757, CVE-2024-36953, CVE-2024-46756, CVE-2024-38596, CVE-2023-52612, CVE-2024-38637, CVE-2024-41071, CVE-2024-46759, CVE-2024-43882, CVE-2024-26675, CVE-2024-43854, CVE-2024-44942, CVE-2024-44998, CVE-2024-42240, CVE-2024-41089, CVE-2024-26636, CVE-2024-46738, CVE-2024-42309)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7121-1>

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-2022-48733
CVE	CVE-2022-48938
CVE	CVE-2022-48943
CVE	CVE-2023-52502
CVE	CVE-2023-52531
CVE	CVE-2023-52578
CVE	CVE-2023-52599
CVE	CVE-2023-52612
CVE	CVE-2023-52614
CVE	CVE-2023-52639
CVE	CVE-2024-26633
CVE	CVE-2024-26636
CVE	CVE-2024-26668
CVE	CVE-2024-26675
CVE	CVE-2024-27397
CVE	CVE-2024-35877
CVE	CVE-2024-36020
CVE	CVE-2024-36953
CVE	CVE-2024-38538
CVE	CVE-2024-38560
CVE	CVE-2024-38596
CVE	CVE-2024-38637
CVE	CVE-2024-41059
CVE	CVE-2024-41071
CVE	CVE-2024-41089
CVE	CVE-2024-41095
CVE	CVE-2024-42094
CVE	CVE-2024-42104
CVE	CVE-2024-42240
CVE	CVE-2024-42309
CVE	CVE-2024-42310
CVE	CVE-2024-43854
CVE	CVE-2024-43882
CVE	CVE-2024-44942
CVE	CVE-2024-44987
CVE	CVE-2024-44998
CVE	CVE-2024-46722
CVE	CVE-2024-46723

CVE	CVE-2024-46738
CVE	CVE-2024-46743
CVE	CVE-2024-46756
CVE	CVE-2024-46757
CVE	CVE-2024-46758
CVE	CVE-2024-46759
CVE XREF	CVE-2024-46800 USN:7121-1

Plugin Information

Published: 2024/11/20, Modified: 2024/11/20

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-231-generic for this advisory.

213508 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7185-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7185-1 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)

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)

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;
- I2C subsystem;
- InfiniBand drivers;
- IRQ chip drivers;
- Network drivers;
- Pin controllers subsystem;
- S/390 drivers;
- TTY drivers;
- USB Host Controller drivers;
- USB Mass Storage drivers;
- Framebuffer layer;
- Ext4 file system;
- File systems infrastructure;
- Bluetooth subsystem;
- DMA mapping infrastructure;
- Memory management;

- 9P file system network protocol;

- IPv4 networking;

- IPv6 networking;

- Logical Link layer;

- MAC80211 subsystem;

- Netfilter;

- NFC subsystem;

- Phonet protocol;

- Network traffic control;

- VMware vSockets driver;

- Wireless networking; (CVE-2024-42090, CVE-2024-42156, CVE-2021-47082, CVE-2024-26921, CVE-2023-52594, CVE-2024-36968, CVE-2024-38633, CVE-2024-42077, CVE-2021-47076, CVE-2021-47501, CVE-2023-52507, CVE-2024-42153, CVE-2024-39301, CVE-2024-36946, CVE-2024-43884, CVE-2023-52509, CVE-2024-36004, CVE-2023-52486, CVE-2024-50264, CVE-2024-45006, CVE-2024-36941, CVE-2024-43856, CVE-2024-40912, CVE-2024-49967, CVE-2024-53057, CVE-2024-26777, CVE-2024-36270, CVE-2024-26625, CVE-2024-45021, CVE-2024-35886, CVE-2024-44947, CVE-2024-44944, CVE-2024-35847, CVE-2024-40959, CVE-2024-42101, CVE-2024-38619)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7185-1>

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-2021-47076
CVE	CVE-2021-47082
CVE	CVE-2021-47501
CVE	CVE-2022-36402
CVE	CVE-2023-35827
CVE	CVE-2023-52486
CVE	CVE-2023-52507
CVE	CVE-2023-52509
CVE	CVE-2023-52594
CVE	CVE-2024-26625
CVE	CVE-2024-26777
CVE	CVE-2024-26921
CVE	CVE-2024-35847
CVE	CVE-2024-35886
CVE	CVE-2024-36004
CVE	CVE-2024-36270
CVE	CVE-2024-36941
CVE	CVE-2024-36946
CVE	CVE-2024-36968

CVE	CVE-2024-38619
CVE	CVE-2024-38633
CVE	CVE-2024-39301
CVE	CVE-2024-40912
CVE	CVE-2024-40959
CVE	CVE-2024-42077
CVE	CVE-2024-42090
CVE	CVE-2024-42101
CVE	CVE-2024-42153
CVE	CVE-2024-42156
CVE	CVE-2024-43856
CVE	CVE-2024-43884
CVE	CVE-2024-44944
CVE	CVE-2024-44947
CVE	CVE-2024-45006
CVE	CVE-2024-45021
CVE	CVE-2024-49967
CVE	CVE-2024-50264
XREF	CVE-2024-53057 USN:7185-1

Plugin Information

Published: 2025/01/06, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-232-generic for this advisory.

214739 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7233-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7233-1 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:

- Multiple devices driver;
- Network drivers;
- Mellanox network drivers;
- S/390 drivers;
- SCSI subsystem;
- Sonic Silicon Backplane drivers;
- File systems infrastructure;
- Closures library;
- Netfilter;
- TIPC protocol;
- VMware vSockets driver; (CVE-2024-26929, CVE-2024-40982, CVE-2024-42311, CVE-2024-53141, CVE-2024-41066, CVE-2024-38661, CVE-2024-38553, CVE-2024-43914, CVE-2024-26663, CVE-2024-42252, CVE-2024-38597, CVE-2024-53103, CVE-2024-41020, CVE-2024-41012, CVE-2024-26595)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

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-2024-26595
CVE	CVE-2024-26663
CVE	CVE-2024-26929
CVE	CVE-2024-38553
CVE	CVE-2024-38597
CVE	CVE-2024-38661
CVE	CVE-2024-40982
CVE	CVE-2024-41012
CVE	CVE-2024-41020
CVE	CVE-2024-41066
CVE	CVE-2024-42252
CVE	CVE-2024-42311
CVE	CVE-2024-43914
CVE	CVE-2024-53103
CVE	CVE-2024-53141
XREF	USN:7233-1

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-233-generic for this advisory.

232628 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7342-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7342-1 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;
- GPIO subsystem;

- GPU drivers;
- Media drivers;
- Network drivers;
- SCSI subsystem;
- Direct Digital Synthesis drivers;
- TTY drivers;
- 9P distributed file system;
- JFS file system;
- NILFS2 file system;
- File systems infrastructure;
- BPF subsystem;
- Netfilter;
- Memory management;
- Amateur Radio drivers;
- B.A.T.M.A.N. meshing protocol;
- Bluetooth subsystem;
- Ethernet bridge;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Open vSwitch;
- Network traffic control;
- TIPC protocol;

- Wireless networking: (CVE-2024-36886, CVE-2024-44931, CVE-2024-50117, CVE-2024-35896, CVE-2024-50229, CVE-2024-40981, CVE-2022-48772, CVE-2024-49902, CVE-2024-53164, CVE-2024-41063, CVE-2024-50233, CVE-2024-36952, CVE-2024-43892, CVE-2024-36964, CVE-2024-43900, CVE-2023-52799, CVE-2024-44938, CVE-2024-40910, CVE-2024-26685, CVE-2024-41064, CVE-2024-43863, CVE-2023-52818, CVE-2024-38567, CVE-2024-53156, CVE-2023-52522, CVE-2024-50134, CVE-2024-40911, CVE-2024-40943, CVE-2024-50148, CVE-2024-42068, CVE-2024-53104, CVE-2023-52880, CVE-2024-42070, CVE-2024-38558, CVE-2023-52488, CVE-2024-43893, CVE-2024-50171)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7342-1>

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-2022-48772
CVE CVE-2023-52488
CVE CVE-2023-52522
CVE CVE-2023-52799
CVE CVE-2023-52818
CVE CVE-2023-52880
CVE CVE-2024-23848
CVE CVE-2024-26685
CVE CVE-2024-35896
CVE CVE-2024-36886
CVE CVE-2024-36952
CVE CVE-2024-36964
CVE CVE-2024-38558
CVE CVE-2024-38567
CVE CVE-2024-40910
CVE CVE-2024-40911
CVE CVE-2024-40943
CVE CVE-2024-40981
CVE CVE-2024-41063
CVE CVE-2024-41064
CVE CVE-2024-42068
CVE CVE-2024-42070
CVE CVE-2024-43863
CVE CVE-2024-43892
CVE CVE-2024-43893
CVE CVE-2024-43900
CVE CVE-2024-44931
CVE CVE-2024-44938
CVE CVE-2024-49902
CVE CVE-2024-50117
CVE CVE-2024-50134
CVE CVE-2024-50148
CVE CVE-2024-50171
CVE CVE-2024-50229
CVE CVE-2024-50233
CVE CVE-2024-53104
CVE CVE-2024-53156
CVE CVE-2024-53164
XREF CISA-KNOWN-EXPLOITED:2025/02/26
XREF USN:7342-1

Plugin Information

Published: 2025/03/11, Modified: 2025/03/11

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-235-generic for this advisory.

235462 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7496-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7496-1 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:

- Block layer subsystem;

- Character device driver;
- Hardware crypto device drivers;
- GPU drivers;
- Media drivers;
- Network drivers;
- SCSI subsystem;
- USB Gadget drivers;
- Framebuffer layer;
- Ceph distributed file system;
- File systems infrastructure;
- JFS file system;
- Network file system (NFS) client;
- NILFS2 file system;
- SMB network file system;
- Netfilter;
- CAN network layer;
- IPv6 networking;
- MAC80211 subsystem;
- Netlink;
- Network traffic control;
- SCTP protocol;
- TIPC protocol; (CVE-2024-53173, CVE-2024-26689, CVE-2024-46771, CVE-2024-36934, CVE-2023-52458, CVE-2021-47191, CVE-2024-50296, CVE-2024-26974, CVE-2021-47150, CVE-2024-53140, CVE-2025-21971, CVE-2024-50237, CVE-2024-46780, CVE-2023-52741, CVE-2024-56642, CVE-2024-56631, CVE-2024-53063, CVE-2024-36015, CVE-2021-47163, CVE-2024-56651, CVE-2024-49925, CVE-2023-52664, CVE-2021-47219, CVE-2024-50256, CVE-2024-53066, CVE-2024-49944, CVE-2024-56598, CVE-2024-56650, CVE-2024-26996, CVE-2024-35864, CVE-2024-56770, CVE-2024-26915, CVE-2023-52927)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7496-1>

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

References

CVE	CVE-2021-47150
CVE	CVE-2021-47163
CVE	CVE-2021-47191
CVE	CVE-2021-47219
CVE	CVE-2023-52458
CVE	CVE-2023-52664
CVE	CVE-2023-52741
CVE	CVE-2023-52927
CVE	CVE-2024-26689
CVE	CVE-2024-26915
CVE	CVE-2024-26974
CVE	CVE-2024-26996
CVE	CVE-2024-35864
CVE	CVE-2024-36015
CVE	CVE-2024-36934
CVE	CVE-2024-46771
CVE	CVE-2024-4680
CVE	CVE-2024-49925
CVE	CVE-2024-49944
CVE	CVE-2024-50237
CVE	CVE-2024-50256
CVE	CVE-2024-50296
CVE	CVE-2024-53063
CVE	CVE-2024-53066
CVE	CVE-2024-53140
CVE	CVE-2024-53173
CVE	CVE-2024-56598
CVE	CVE-2024-56631
CVE	CVE-2024-56642
CVE	CVE-2024-56650
CVE	CVE-2024-56651
CVE	CVE-2024-56770
CVE	CVE-2025-21971
XREF	USN:7496-1

Plugin Information

Published: 2025/05/07, Modified: 2025/05/07

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-237-generic for this advisory.

237867 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7553-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7553-1 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:

- Clock framework and drivers;
- GPU drivers;
- Parport drivers;
- Ext4 file system;
- JFFS2 file system;
- JFS file system;

- File systems infrastructure;

- Sun RPC protocol;

- USB sound devices; (CVE-2024-42301, CVE-2024-53168, CVE-2024-47701, CVE-2021-47211, CVE-2024-53155, CVE-2024-56596, CVE-2024-26966, CVE-2024-56551, CVE-2024-57850)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7553-1>

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-2024-26966
CVE	CVE-2024-42301
CVE	CVE-2024-47701
CVE	CVE-2024-53155
CVE	CVE-2024-53168
CVE	CVE-2024-56551
CVE	CVE-2024-56596
CVE	CVE-2024-57850
XREF	USN:7553-1

Plugin Information

Published: 2025/06/05, Modified: 2025/06/05

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-238-generic for this advisory.

243968 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7685-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7685-1 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:

- Device tree and open firmware driver;
 - SCSI subsystem;
 - TTY drivers;
 - Ext4 file system;
 - SMB network file system;
 - Bluetooth subsystem;
 - Network traffic control;
 - Sun RPC protocol;
- USB sound devices; (CVE-2024-53239, CVE-2023-52975, CVE-2024-38541, CVE-2023-52885, CVE-2024-49883, CVE-2025-37797, CVE-2023-52757, CVE-2024-56748, CVE-2024-49950, CVE-2024-50073)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7685-1>

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-2023-52757
CVE	CVE-2023-52885
CVE	CVE-2023-52975
CVE	CVE-2024-38541
CVE	CVE-2024-49883
CVE	CVE-2024-49950
CVE	CVE-2024-50073
CVE	CVE-2024-53239
CVE	CVE-2024-56748
XREF	CVE-2025-37797 USN:7685-1

Plugin Information

Published: 2025/08/06, Modified: 2025/08/06

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-240-generic for this advisory.

145518 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability (USN-4710-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4710-1 advisory.

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).

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4710-1>

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

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
XREF [CVE-2020-25704](#)
[USN:4710-1](#)

Plugin Information

Published: 2021/01/28, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-133-generic for this advisory.

216769 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability (USN-7296-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7296-1 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7296-1>

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

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2025-0927
XREF	USN:7296-1

Plugin Information

Published: 2025/02/25, Modified: 2025/02/25

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-234-generic for this advisory.

126772 - Ubuntu 16.04 LTS / 18.04 LTS : NSS vulnerabilities (USN-4060-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4060-1 advisory.

Henry Corrigan-Gibbs discovered that NSS incorrectly handled importing certain curve25519 private keys. An attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2019-11719)

Hubert Kario discovered that NSS incorrectly handled PKCS#1 v1.5 signatures when using TLSv1.3. An attacker could possibly use this issue to trick NSS into using PKCS#1 v1.5 signatures, contrary to expectations. This issue only applied to Ubuntu 19.04. (CVE-2019-11727)

Jonas Altmann discovered that NSS incorrectly handled certain p256-ECDH public keys. An attacker could possibly use this issue to cause NSS to crash, resulting in a denial of service. (CVE-2019-11729)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4060-1>

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

6.5 (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-2019-11719
CVE	CVE-2019-11727
XREF	CVE-2019-11729

Plugin Information

Published: 2019/07/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3 2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.6
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.6

131559 - Ubuntu 16.04 LTS / 18.04 LTS : NSS vulnerability (USN-4203-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4203-1 advisory.

It was 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4203-1>

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-2019-11745
XREF	USN:4203-1

Plugin Information

Published: 2019/12/03, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.8
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.8

131923 - Ubuntu 16.04 LTS / 18.04 LTS : NSS vulnerability (USN-4215-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4215-1 advisory.

It was discovered that NSS incorrectly handled certain certificates. 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-4215-1>

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-2019-17007
XREF	USN:4215-1

Plugin Information

Published: 2019/12/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.9
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.9

183630 - Ubuntu 16.04 LTS / 18.04 LTS : NTFS-3G vulnerability (USN-3914-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3914-1 advisory.

A heap buffer overflow was discovered in NTFS-3G when executing it with a relative mount point path that is too long. A local attacker could potentially exploit this to execute arbitrary code as the 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-3914-1>

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

6.1 (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-2019-9755
XREF	USN:3914-1

Plugin Information

Published: 2023/10/21, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g_1:2015.3.14AR.1-1ubuntu0.2

207999 - Ubuntu 16.04 LTS / 18.04 LTS : ORC vulnerability (USN-6964-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6964-2 advisory.

USN-6964-1 fixed a vulnerability in ORC. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 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-6964-2>

Solution

Update the affected liborc-0.4-0, liborc-0.4-dev and / or liborc-0.4-dev-bin 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 (CVSS:2.0/AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.4 (CVSS:2.0/E:U/RL:OF/RC:C)

References

CVE-2024-40897
XREF USN:6964-2

Plugin Information

Published: 2024/10/01, Modified: 2024/10/01

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 : liborc-0.4-0_1:0.4.25-1
- Fixed package : liborc-0.4-0_1:0.4.25-1ubuntu0.1~esm1

129712 - Ubuntu 16.04 LTS / 18.04 LTS : OpenEXR vulnerabilities (USN-4148-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4148-1 advisory.

It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-12596)

Brandon Perry discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-9110, CVE-2017-9112, CVE-2017-9116)

Brandon Perry discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. (CVE-2017-9111, CVE-2017-9113, CVE-2017-9115)

Tan Jie discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. (CVE-2018-18444)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4148-1>

Solution

Update the affected libopenexr-dev, libopenexr22 and / or openexr 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-2017-12596
CVE	CVE-2017-9110
CVE	CVE-2017-9111
CVE	CVE-2017-9112
CVE	CVE-2017-9113
CVE	CVE-2017-9115
CVE	CVE-2017-9116
CVE	CVE-2018-18444
XREF	USN:4148-1

Plugin Information

Published: 2019/10/08, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.1
```

127794 - Ubuntu 16.04 LTS / 18.04 LTS : OpenLDAP vulnerabilities (USN-4078-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4078-1 advisory.

It was discovered that OpenLDAP incorrectly handled rootDN delegation. A database administrator could use this issue to request authorization as an identity from another database, contrary to expectations.

(CVE-2019-13057)

It was discovered that OpenLDAP incorrectly handled SASL authentication and session encryption. After a first SASL bind was completed, it was possible to obtain access by performing simple binds, contrary to expectations. (CVE-2019-13565)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4078-1>

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

6.5 (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)

References

CVE	CVE-2019-13057
CVE	CVE-2019-13565
XREF	USN:4078-1

Plugin Information

Published: 2019/08/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.4
- Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.6

136967 - Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4376-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4376-1 advisory.

Cesar Pereida Garca, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, and Billy Brumley discovered that OpenSSL incorrectly handled ECDSA signatures. An attacker could possibly use this issue to perform a timing side-channel attack and recover private ECDSA keys. (CVE-2019-1547)

Matt Caswell discovered that OpenSSL incorrectly handled the random number generator (RNG). This may result in applications that use the fork() system call sharing the same RNG state between the parent and the child, contrary to expectations. This issue only affected Ubuntu 18.04 LTS and Ubuntu 19.10. (CVE-2019-1549)

Guido Vranken discovered that OpenSSL incorrectly performed the x86_64 Montgomery squaring procedure. While unlikely, a remote attacker could possibly use this issue to recover private keys. (CVE-2019-1551)

Bernd Edlinger discovered that OpenSSL incorrectly handled certain decryption functions. In certain scenarios, a remote attacker could possibly use this issue to perform a padding oracle attack and decrypt traffic. (CVE-2019-1563)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

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-2019-1547
CVE	CVE-2019-1549
CVE	CVE-2019-1551
CVE	CVE-2019-1563
XREF	USN:4376-1

Plugin Information

Published: 2020/05/29, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.16
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.16

140645 - Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4504-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4504-1 advisory.

Robert Merget, Marcus Brinkmann, Nimrod Aviram, and Juraj Somorovsky discovered that certain Diffie-Hellman ciphersuites in the TLS specification and implemented by OpenSSL contained a flaw. A remote attacker could possibly use this issue to eavesdrop on encrypted communications. This was fixed in this update by removing the insecure ciphersuites from OpenSSL. (CVE-2020-1968)

Cesar Pereida Garca, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, and Billy Brumley discovered that OpenSSL incorrectly handled ECDSA signatures. An attacker could possibly use this issue to perform a timing side-channel attack and recover private ECDSA keys. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-1547)

Guido Vranken discovered that OpenSSL incorrectly performed the x86_64 Montgomery squaring procedure.

While unlikely, a remote attacker could possibly use this issue to recover private keys. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-1551)

Bernd Edlinger discovered that OpenSSL incorrectly handled certain decryption functions. In certain scenarios, a remote attacker could possibly use this issue to perform a padding oracle attack and decrypt traffic. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-1563)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4504-1>

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-2019-1547
CVE	CVE-2019-1551
CVE	CVE-2019-1563
CVE	CVE-2020-1968
XREF	USN:4504-1
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/09/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.17
- Installed package : openssl 1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.17

190449 - Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-6632-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6632-1 advisory.

David Benjamin discovered that OpenSSL incorrectly handled excessively long X9.42 DH keys. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2023-5678)

Baha Naamneh discovered that OpenSSL incorrectly handled certain malformed PKCS12 files. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service.

(CVE-2024-0727)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6632-1>

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

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-5678
CVE	CVE-2024-0727
XREF	USN:6632-1
XREF	IAVA:2024-A-0121-S

Plugin Information

Published: 2024/02/13, 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.

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm11
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm11

122500 - Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerability (USN-3899-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3899-1 advisory.

Juraj Somorovsky, Robert Merget, and Nimrod Aviram discovered that certain applications incorrectly used OpenSSL and could be exposed to a padding oracle attack. A remote attacker could possibly use this issue to decrypt 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-3899-1>

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	CVE-2019-1559
XREF	USN:3899-1
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2019/02/28, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.15
- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.15

138874 - Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4430-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4430-1 advisory.

It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted image file, a remote attacker could possibly cause Pillow 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-4430-1>

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-2020-10177
CVE	CVE-2020-10378
CVE	CVE-2020-10994
CVE	CVE-2020-11538
XREF	USN:4430-1

Plugin Information

Published: 2020/07/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-pil_3.1.2-0ubuntu1.1
- Fixed package : python3-pil_3.1.2-0ubuntu1.4

145081 - Ubuntu 16.04 LTS / 18.04 LTS : PyXDG vulnerability (USN-4700-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4700-1 advisory.

Alexandre D'Hondt discovered that PyXDG did not properly sanitize input. An attacker could exploit this with a crafted .menu file 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-4700-1>

Solution

Update the affected python-xdg and / or python3-xdg 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

6.7 (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)

References

CVE	CVE-2019-12761
XREF	USN:4700-1

Plugin Information

Published: 2021/01/19, Modified: 2025/02/20

Plugin Output

tcp/0

- Installed package : python3-xdg_0.25-4

- Fixed package : python3-xdg_0.25-4ubuntu0.16.04.1

128631 - Ubuntu 16.04 LTS / 18.04 LTS : Python vulnerabilities (USN-4127-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4127-1 advisory.

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 16.04 LTS and Ubuntu 18.04 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. (CVE-2018-20852)

Jonathan Birch and Panayiotis Panayiotou discovered that Python incorrectly handled Unicode encoding during NFKC normalization. An attacker could possibly use this issue to obtain sensitive information. (CVE-2019-9636, CVE-2019-10160)

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 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-5010)

It was discovered that Python incorrectly handled certain urls. A remote attacker could possibly use this issue to perform CRLF injection attacks. (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. (CVE-2019-9948)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4127-1>

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

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-20406
CVE	CVE-2018-20852
CVE	CVE-2019-10160
CVE	CVE-2019-5010
CVE	CVE-2019-9636
CVE	CVE-2019-9740
CVE	CVE-2019-9947
CVE	CVE-2019-9948
XREF	USN:4127-1

Plugin Information

Published: 2019/09/10, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.8

- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.8

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.8

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.8

- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.8

- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.8

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.8

- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.8

- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.8

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.8
```

129774 - Ubuntu 16.04 LTS / 18.04 LTS : Python vulnerabilities (USN-4151-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4151-1 advisory.

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.

(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. (CVE-2019-16935)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4151-1>

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)

References

CVE	CVE-2019-16056
CVE	CVE-2019-16935
XREF	USN:4151-1

Plugin Information

Published: 2019/10/10, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.9
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.9
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.9
- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.9
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.9
- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.9
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.9
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.9
- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.9
- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.9

135894 - Ubuntu 16.04 LTS / 18.04 LTS : Python vulnerabilities (USN-4333-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4333-1 advisory.

It was discovered that Python incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. (CVE-2019-18348)

It was discovered that Python incorrectly handled certain HTTP requests. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-8492)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4333-1>

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

5.5 (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-2019-18348
CVE	CVE-2020-8492
XREF	USN:4333-1

Plugin Information

Published: 2020/04/22, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.11

- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.11

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.11

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.10
- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.10

- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.10

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.11

- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.11

- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.10

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.10
```

141459 - Ubuntu 16.04 LTS / 18.04 LTS : Python vulnerability (USN-4581-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4581-1 advisory.

It was discovered that Python 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-4581-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.2 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

6.5 (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-2020-26116
XREF	USN:4581-1

Plugin Information

Published: 2020/10/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.13

- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.13

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.13

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.12

- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.12

- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.5
- Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.12

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.13

- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.13

- Installed package : python3.5_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5_3.5.2-2ubuntu0~16.04.12

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.5
- Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.12
```

133647 - Ubuntu 16.04 LTS / 18.04 LTS : Qt vulnerabilities (USN-4275-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4275-1 advisory.

It was discovered that Qt incorrectly handled certain PPM images. If a user or automated system were tricked into opening a specially crafted PPM file, a remote attacker could cause Qt to crash, resulting in a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-19872)

It was discovered that Qt incorrectly handled certain text files. If a user or automated system were tricked into opening a specially crafted text file, a remote attacker could cause Qt to crash, resulting in a denial of service. This issue only affected Ubuntu 19.10. (CVE-2019-18281)

It was discovered that Qt incorrectly searched for plugins in the current working directory. An attacker could possibly use this issue to execute arbitrary code. (CVE-2020-0569)

It was discovered that Qt incorrectly searched for libraries relative to the current working directory. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 19.10.
(CVE-2020-0570)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4275-1>

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

6.6 (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-2018-19872
CVE	CVE-2019-18281
CVE	CVE-2020-0569
CVE XREF	CVE-2020-0570 USN:4275-1

Plugin Information

Published: 2020/02/12, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libqt5core5a_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5core5a_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5dbus5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5dbus5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5gui5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5gui5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5network5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5network5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5opengl5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5opengl5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5printsupport5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5printsupport5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5sql5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5sql5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5sql5-sqlite_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5sql5-sqlite_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5test5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5test5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5widgets5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5widgets5_5.5.1+dfsg-16ubuntu7.7

- Installed package : libqt5xml5_5.5.1+dfsg-16ubuntu7.5
- Fixed package : libqt5xml5_5.5.1+dfsg-16ubuntu7.7
```

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4205-1 advisory.

It was discovered that SQLite incorrectly handled certain schemas. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 12.04 ESM. (CVE-2018-8740)

It was discovered that SQLite incorrectly handled certain schemas. 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 19.04. (CVE-2019-16168)

It was discovered that SQLite incorrectly handled certain schemas. An attacker could possibly use this issue to mishandles some expressions. This issue only affected Ubuntu 19.04 and Ubuntu 19.10.
(CVE-2019-19242)

It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 19.04 and Ubuntu 19.10. (CVE-2019-19244)

It was discovered that SQLite incorrectly handled certain SQL commands. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 19.04. (CVE-2019-5018)

It was discovered that SQLite incorrectly handled certain commands. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-5827)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4205-1>

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-2018-8740
CVE	CVE-2019-16168
CVE	CVE-2019-19242
CVE	CVE-2019-19244
CVE	CVE-2019-5018
CVE	CVE-2019-5827
XREF	USN:4205-1

Plugin Information

Published: 2019/12/03, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libsqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.3

134402 - Ubuntu 16.04 LTS / 18.04 LTS : SQLite vulnerabilities (USN-4298-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4298-1 advisory.

It was discovered that SQLite incorrectly handled certain shadow tables. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2019-13734, CVE-2019-13750, CVE-2019-13753)

It was discovered that SQLite incorrectly handled certain corrupt records. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2019-13751)

It was discovered that SQLite incorrectly handled certain queries. 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 19.10. (CVE-2019-19880)

It was discovered that SQLite incorrectly handled certain queries. 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 18.04 LTS and Ubuntu 19.10. (CVE-2019-19923)

It was discovered that SQLite incorrectly handled parser tree rewriting. 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 19.10. (CVE-2019-19924)

It was discovered that SQLite incorrectly handled certain ZIP archives. 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 18.04 LTS and Ubuntu 19.10. (CVE-2019-19925, CVE-2019-19959)

It was discovered that SQLite incorrectly handled errors during parsing. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2019-19926)

It was discovered that SQLite incorrectly handled parsing errors. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2019-20218)

It was discovered that SQLite incorrectly handled generated column optimizations. 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 18.04 LTS and Ubuntu 19.10. (CVE-2020-9327)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4298-1>

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:O/RC:C)

References

CVE	CVE-2019-13734
CVE	CVE-2019-13750
CVE	CVE-2019-13751
CVE	CVE-2019-13752
CVE	CVE-2019-13753
CVE	CVE-2019-19880
CVE	CVE-2019-19923
CVE	CVE-2019-19924
CVE	CVE-2019-19925
CVE	CVE-2019-19926
CVE	CVE-2019-19959
CVE	CVE-2019-20218
XREF	CVE-2020-9327 USN:4298-1

Plugin Information

Published: 2020/03/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libsqlite3-0_3.11.0-1ubuntu1.1
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.4
```

133449 - Ubuntu 16.04 LTS / 18.04 LTS : Sudo vulnerability (USN-4263-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4263-1 advisory.

Joe Vennix discovered that Sudo incorrectly handled memory operations when the pwfeedback option is enabled. A local attacker could possibly use this issue to obtain unintended access to the administrator account.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4263-1>

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

7.0 (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-2019-18634
XREF	USN:4263-1

Plugin Information

Plugin Output

tcp/0

- Installed package : sudo_1.8.16-0ubuntu1.5
- Fixed package : sudo_1.8.16-0ubuntu1.9

183639 - Ubuntu 16.04 LTS / 18.04 LTS : Vim vulnerabilities (USN-4582-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4582-1 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 16.04 LTS.

(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. (CVE-2019-20807)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4582-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/U: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:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2017-17087
CVE	CVE-2019-20807
XREF	IAVB:2020-B-0053-S
XREF	USN:4582-1

Plugin Information

Published: 2023/10/21, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : vim 2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5

- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5

- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5
```

126568 - Ubuntu 16.04 LTS / 18.04 LTS : Whoopsie vulnerability (USN-4052-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4052-1 advisory.

Kevin Backhouse discovered Whoopsie incorrectly handled very large crash reports. A local attacker could possibly use this issue to cause a denial of service 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-4052-1>

Solution

Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie 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-2019-11476
XREF	USN:4052-1

Plugin Information

Published: 2019/07/09, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libwhoopsie0_0.2.52.5
- Fixed package : libwhoopsie0_0.2.52.5ubuntu0.1

- Installed package : whoopsie_0.2.52.5
- Fixed package : whoopsie_0.2.52.5ubuntu0.1
```

130395 - Ubuntu 16.04 LTS / 18.04 LTS : Whoopsie vulnerability (USN-4170-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4170-1 advisory.

Kevin Backhouse discovered Whoopsie incorrectly handled very large crash reports. A local attacker could possibly use this issue to cause a denial of service, expose sensitive information or execute code as the whoopsie 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-4170-1>

Solution

Update the affected libwhoopsie-dev, libwhoopsie0 and / or whoopsie 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-2019-11484
XREF	USN:4170-1

Plugin Information

Published: 2019/10/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libwhoopsie0_0.2.52.5
- Fixed package : libwhoopsie0_0.2.52.5ubuntu0.2
- Installed package : whoopsie_0.2.52.5
- Fixed package : whoopsie_0.2.52.5ubuntu0.2

232549 - Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerabilities (USN-7299-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7299-2 advisory.

USN-7299-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-7299-2>

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

6.0 (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

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	IAVA:2025-A-0135
XREF	USN:7299-2

Plugin Information

Published: 2025/03/10, Modified: 2025/03/10

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm15
- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm7
- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm7

209909 - Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerability (USN-7085-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7085-2 advisory.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7085-2>

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-2024-9632
XREF	USN:7085-2 IAVA:2025-A-0135

Plugin Information

Published: 2024/10/30, Modified: 2025/02/28

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.

```
- Installed package : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm14

- Installed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-core-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm6

- Installed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.2
- Fixed package : xserver-xorg-legacy-hwe-16.04_2:1.19.6-1ubuntu4.1~16.04.6+esm6
```

125355 - Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerabilities (USN-3993-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3993-1 advisory.

Wenchao Li discovered that curl incorrectly handled memory in the curl_url_set() function. 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 19.04. (CVE-2019-5435)

It was discovered that curl incorrectly handled memory when receiving data from a TFTP 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-2019-5436)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3993-1>

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-2019-5435
CVE	CVE-2019-5436
XREF	USN:3993-1

Plugin Information

Published: 2019/05/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.13
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.13

190689 - Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6641-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6641-1 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6641-1>

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/C:H/VI:H/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
XREF	IAVA:2023-A-0674-S
XREF	USN:6641-1

Plugin Information

Published: 2024/02/19, 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.

- Installed package : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm11
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm11

129488 - Ubuntu 16.04 LTS / 18.04 LTS : e2fsprogs vulnerability (USN-4142-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4142-1 advisory.

It was discovered that e2fsprogs incorrectly handled certain ext4 partitions. 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-4142-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/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

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-2019-5094
XREF	USN:4142-1

Plugin Information

Published: 2019/10/01, Modified: 2025/06/02

Plugin Output

tcp/0

- Installed package : e2fslibs_1.42.13-1ubuntu1
- Fixed package : e2fslibs_1.42.13-1ubuntu1.1
- Installed package : e2fsprogs_1.42.13-1ubuntu1
- Fixed package : e2fsprogs_1.42.13-1ubuntu1.1
- Installed package : libcomerr2_1.42.13-1ubuntu1
- Fixed package : libcomerr2_1.42.13-1ubuntu1.1
- Installed package : libss2_1.42.13-1ubuntu1
- Fixed package : libss2_1.42.13-1ubuntu1.1

133225 - Ubuntu 16.04 LTS / 18.04 LTS : e2fsprogs vulnerability (USN-4249-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4249-1 advisory.

It was discovered that e2fsprogs incorrectly handled certain ext4 partitions. 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-4249-1>

Solution

Update the affected packages.

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/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-2019-5188
XREF	USN:4249-1

Plugin Information

Published: 2020/01/24, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : e2fslibs_1.42.13-1ubuntu1
- Fixed package : e2fslibs_1.42.13-1ubuntu1.2
- Installed package : e2fsprogs_1.42.13-1ubuntu1
- Fixed package : e2fsprogs_1.42.13-1ubuntu1.2

- Installed package : libcomerr2_1.42.13-1ubuntu1
- Fixed package : libcomerr2_1.42.13-1ubuntu1.2

- Installed package : libss2_1.42.13-1ubuntu1
- Fixed package : libss2_1.42.13-1ubuntu1.2

122946 - Ubuntu 16.04 LTS / 18.04 LTS : file vulnerabilities (USN-3911-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3911-1 advisory.

It was discovered that file incorrectly handled certain malformed ELF files. 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3911-1>

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-2019-8904
CVE	CVE-2019-8905
CVE	CVE-2019-8906
CVE	CVE-2019-8907
XREF	USN:3911-1

Plugin Information

Published: 2019/03/19, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : file_1:5.25-2ubuntu1.1
- Fixed package : file_1:5.25-2ubuntu1.2
- Installed package : libmagical_1:5.25-2ubuntu1.1
- Fixed package : libmagical_1:5.25-2ubuntu1.2

130428 - Ubuntu 16.04 LTS / 18.04 LTS : file vulnerability (USN-4172-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4172-1 advisory.

It was discovered that file incorrectly handled certain malformed files. 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-4172-1>

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-2019-18218
XREF	USN:4172-1

Plugin Information

Published: 2019/10/31, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : file_1:5.25-2ubuntu1.1
- Fixed package : file_1:5.25-2ubuntu1.3

- Installed package : libmagic1_1:5.25-2ubuntu1.1
- Fixed package : libmagic1_1:5.25-2ubuntu1.3
```

134298 - Ubuntu 16.04 LTS / 18.04 LTS : libarchive vulnerabilities (USN-4293-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4293-1 advisory.

It was discovered that libarchive incorrectly handled certain archive files. An attacker could possibly use this issue to access sensitive information. (CVE-2019-19221)

It was discovered that libarchive incorrectly handled certain archive files. An attacker could possibly use this issue to cause a crash resulting in a denial of service or possibly unspecified other impact.

This issue only affected Ubuntu 19.10. (CVE-2020-9308)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4293-1>

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-2019-19221
CVE	CVE-2020-9308
XREF	USN:4293-1

Plugin Information

Published: 2020/03/06, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libarchive13_3.1.2-11ubuntu0.16.04.6
- Fixed package : libarchive13_3.1.2-11ubuntu0.16.04.8
```

130394 - Ubuntu 16.04 LTS / 18.04 LTS : libarchive vulnerability (USN-4169-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4169-1 advisory.

It was discovered that libarchive incorrectly handled certain archive files. An attacker could 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-4169-1>

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-2019-18408
XREF	USN:4169-1

Plugin Information

Published: 2019/10/30, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libarchive13_3.1.2-11ubuntu0.16.04.6
- Fixed package : libarchive13_3.1.2-11ubuntu0.16.04.7

133649 - Ubuntu 16.04 LTS / 18.04 LTS : libexif vulnerabilities (USN-4277-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4277-1 advisory.

Liu Bingchang discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information or cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2016-6328)

Lili Xu and Bingchang Liu discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information or cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2017-7544)

It was discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-9278)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4277-1>

Solution

Update the affected libexif-dev and / or libexif12 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)

CVSS v3.0 Temporal Score

8.2 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (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-2016-6328
CVE	CVE-2017-7544
CVE	CVE-2019-9278
XREF	USN:4277-1

Plugin Information

Published: 2020/02/12, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : libexif12_0.6.21-2
- Fixed package : libexif12_0.6.21-2ubuntu0.1

132016 - Ubuntu 16.04 LTS / 18.04 LTS : libpcap vulnerability (USN-4221-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4221-1 advisory.

It was discovered that libpcap did not properly validate PHB headers in some situations. An attacker could use this to cause a denial of service (memory exhaustion).

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4221-1>

Solution

Update the affected libpcap-dev, libpcap0.8 and / or libpcap0.8-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: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)

References

CVE	CVE-2019-15165
XREF	USN:4221-1

Plugin Information

Published: 2019/12/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpcap0.8_1.7.4-2
- Fixed package : libpcap0.8_1.7.4-2ubuntu0.1

139180 - Ubuntu 16.04 LTS / 18.04 LTS : librsvg regression (USN-4436-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4436-2 advisory.

USN-4436-1 fixed a vulnerability in librsvg. The upstream fix caused a regression when parsing certain SVG files. This update backs out the fix pending further investigation.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4436-2>

Solution

Update the affected packages.

Risk Factor

Medium

References

XREF	USN:4436-2
------	------------

Plugin Information

Published: 2020/07/30, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : librsvg2-2_2.40.13-3
- Fixed package : librsvg2-2_2.40.13-3ubuntu0.2
- Installed package : librsvg2-common_2.40.13-3
- Fixed package : librsvg2-common_2.40.13-3ubuntu0.2

139024 - Ubuntu 16.04 LTS / 18.04 LTS : librsvg vulnerabilities (USN-4436-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4436-1 advisory.

It was discovered that librsvg incorrectly handled parsing certain SVG files. A remote attacker could possibly use this issue to cause librsvg to crash, resulting in a denial of service. This issue only affected Ubuntu 16.04 LTS. (CVE-2017-11464)

It was discovered that librsvg incorrectly handled parsing certain SVG files with nested patterns. A remote attacker could possibly use this issue to cause librsvg to consume resources and crash, resulting in a denial of service. (CVE-2019-20446)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4436-1>

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-2017-11464
CVE	CVE-2019-20446
XREF	USN:4436-1

Plugin Information

Published: 2020/07/28, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : librsvg2-2_2.40.13-3
- Fixed package : librsvg2-2_2.40.13-3ubuntu0.1
- Installed package : librsvg2-common_2.40.13-3
- Fixed package : librsvg2-common_2.40.13-3ubuntu0.1

125812 - Ubuntu 16.04 LTS / 18.04 LTS : libsndfile vulnerabilities (USN-4013-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4013-1 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4013-1>

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-2017-14245
CVE	CVE-2017-14246
CVE	CVE-2017-14634
CVE	CVE-2017-16942
CVE	CVE-2017-6892
CVE	CVE-2018-13139
CVE	CVE-2018-19432
CVE	CVE-2018-19661
CVE	CVE-2018-19662
CVE	CVE-2018-19758
CVE	CVE-2019-3832
XREF	USN:4013-1

Plugin Information

Published: 2019/06/11, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.2

133646 - Ubuntu 16.04 LTS / 18.04 LTS : libxml2 vulnerabilities (USN-4274-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

11/2/25, 1:18 AM

Photographer

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4274-1 advisory.

It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-19956, CVE-2020-7595)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4274-1>

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-2019-19956
CVE	CVE-2020-7595
XREF	USN:4274-1

Plugin Information

Published: 2020/02/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libxml2_2.9.3+dfsg1-1ubuntu0.6
- Fixed package : libxml2_2.9.3+dfsg1-1ubuntu0.7

143266 - Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4646-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4646-1 advisory.

It was discovered that Poppler incorrectly handled certain files. If a user or automated system were tricked into opening a crafted PDF file, an attacker could 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 these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4646-1>

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

BID	107862
BID	109342
CVE	CVE-2018-21009
CVE	CVE-2019-9959
CVE	CVE-2019-10871
CVE	CVE-2019-13283
CVE	CVE-2020-27778
XREF	USN:4646-1

Plugin Information

Published: 2020/11/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.15
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.15
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.15

213997 - Ubuntu 16.04 LTS / 18.04 LTS : snapd vulnerabilities (USN-6940-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6940-2 advisory.

USN-6940-1 fixed vulnerabilities in snapd. This update provides the

corresponding updates for Ubuntu 18.04 LTS and Ubuntu 16.04 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-6940-2>

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:6940-2

Plugin Information

Published: 2025/01/13, Modified: 2025/01/13

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.

- Installed package : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.61.4ubuntu0.16.04.1+esm1
- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.61.4ubuntu0.16.04.1+esm1

133523 - Ubuntu 16.04 LTS / 18.04 LTS : systemd vulnerabilities (USN-4269-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4269-1 advisory.

It was discovered that systemd incorrectly handled certain PIDFile files. A local attacker could possibly use this issue to trick systemd into killing privileged processes. This issue only affected Ubuntu 16.04 LTS. (CVE-2018-16888)

It was discovered that systemd incorrectly handled certain udevadm trigger commands. A local attacker could possibly use this issue to cause systemd to consume resources, leading to a denial of service.
(CVE-2019-20386)

Jann Horn discovered that systemd incorrectly handled services that use the DynamicUser property. A local attacker could possibly use this issue to access resources owned by a different service in the future.

This issue only affected Ubuntu 18.04 LTS. (CVE-2019-3843, CVE-2019-3844)

Tavis Ormandy discovered that systemd incorrectly handled certain Polkit queries. A local attacker could use this issue to cause systemd to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges. (CVE-2020-1712)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4269-1>

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-2018-16888
CVE	CVE-2019-20386
CVE	CVE-2019-3843
CVE	CVE-2019-3844
CVE	CVE-2020-1712
XREF	USN:4269-1

Plugin Information

Published: 2020/02/06, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libpam-systemd_229-4ubuntu21.16
- Fixed package : libpam-systemd_229-4ubuntu21.27

- Installed package : libsystemd0_229-4ubuntu21.16
- Fixed package : libsystemd0_229-4ubuntu21.27

- Installed package : libudev1_229-4ubuntu21.16
- Fixed package : libudev1_229-4ubuntu21.27

- Installed package : systemd_229-4ubuntu21.16
- Fixed package : systemd_229-4ubuntu21.27

- Installed package : systemd-sysv_229-4ubuntu21.16
- Fixed package : systemd-sysv_229-4ubuntu21.27
- Installed package : udev_229-4ubuntu21.16
- Fixed package : udev_229-4ubuntu21.27
```

144337 - Ubuntu 16.04 LTS / 18.04 LTS : unzip vulnerabilities (USN-4672-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4672-1 advisory.

Rene Freingruber discovered that unzip incorrectly handled certain specially crafted password protected ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. (CVE-2018-1000035)

Antonio Carista discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. (CVE-2018-18384)

It was discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause resource consumption, resulting in a denial of service. (CVE-2019-13232)

Martin Carpenter discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM,

Alexis Vanden Eijnde discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2016-9844)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4672-1>

Solution

Update the affected unzip 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

7.0 (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

BID	94728
BID	95081
CVE	CVE-2014-9913
CVE	CVE-2016-9844
CVE	CVE-2018-18384
CVE	CVE-2018-1000035
CVE	CVE-2019-13232
XREF	USN:4672-1

Plugin Information

Published: 2020/12/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : unzip_6.0-20ubuntu1
- Fixed package : unzip_6.0-20ubuntu1.1
```

125338 - Ubuntu 16.04 LTS / 18.04 LTS : urllib3 vulnerabilities (USN-3990-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3990-1 advisory.

It was discovered that urllib3 incorrectly removed Authorization HTTP headers when handled cross-origin redirects. This could result in credentials being sent to unintended hosts. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 18.10. (CVE-2018-20060)

It was discovered that urllib3 incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. (CVE-2019-11236)

It was discovered that urllib3 incorrectly handled situations where a desired set of CA certificates were specified. This could result in certificates being accepted by

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-3990-1>

Solution

Update the affected python-urllib3 and / or python3-urllib3 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-20060
CVE	CVE-2019-11236
CVE	CVE-2019-11324
XREF	USN:3990-1

Plugin Information

Published: 2019/05/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : python3-urllib3_1.13.1-2ubuntu0.16.04.2
- Fixed package : python3-urllib3_1.13.1-2ubuntu0.16.04.3

124696 - Ubuntu 16.04 LTS / 18.04 LTS : wpa_supplicant and hostapd vulnerability (USN-3969-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3969-1 advisory.

It was discovered that wpa_supplicant and hostapd incorrectly handled unexpected fragments when using EAP- pwd. 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-3969-1>

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

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:O/RC:C)

References

CVE CVE-2019-11555

XREF USN:3969-1

Plugin Information

Published: 2019/05/08, Modified: 2025/03/20

Plugin Output

tcp/0

- Installed package : wpasupplicant_2.4-0ubuntu6.3
- Fixed package : wpasupplicant_2.4-0ubuntu6.5

125767 - Ubuntu 16.04 LTS : AppArmor update (USN-4008-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4008-2 advisory.

USN-4008-1 fixed multiple security issues in the Linux kernel. This update provides the corresponding changes to AppArmor policy for correctly operating under the Linux kernel with fixes for CVE-2019-11190.

Without these changes, some profile transitions may be unintentionally denied due to missing mmap ('m') rules.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4008-2>

Solution

Update the affected packages.

Risk Factor

Medium

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

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-2019-11190
XREF	USN:4008-2

Plugin Information

Published: 2019/06/07, Modified: 2025/03/03

Plugin Output

tcp/0

- Installed package : apparmor_2.10.95-0ubuntu2.10
- Fixed package : apparmor_2.10.95-0ubuntu2.11
- Installed package : libapparmor-perl_2.10.95-0ubuntu2.10
- Fixed package : libapparmor-perl_2.10.95-0ubuntu2.11
- Installed package : libapparmor1_2.10.95-0ubuntu2.10
- Fixed package : libapparmor1_2.10.95-0ubuntu2.11

202245 - Ubuntu 16.04 LTS : Apport vulnerabilities (USN-6894-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6894-1 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 a 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-6894-1>

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	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:6894-1

Plugin Information

Published: 2024/07/12, Modified: 2024/08/29

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 : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30+esm4
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30+esm4
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30+esm4
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30+esm4

216160 - Ubuntu 16.04 LTS : BlueZ vulnerabilities (USN-7265-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7265-1 advisory.

Julian Rauchberger discovered that BlueZ did not correctly handle certain memory operations. An attacker could possibly use this issue to leak sensitive information or execute arbitrary code. (CVE-2019-8921, CVE-2019-8922)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7265-1>

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-2019-8921
CVE-2019-8922
XREF USN:7265-1

Plugin Information

Published: 2025/02/12, Modified: 2025/02/12

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 : bluez_5.37-0ubuntu5.1
- Fixed package : bluez_5.37-0ubuntu5.3+esm5
- Installed package : bluez-cups_5.37-0ubuntu5.1
- Fixed package : bluez-cups_5.37-0ubuntu5.3+esm5
- Installed package : bluez-obexd_5.37-0ubuntu5.1
- Fixed package : bluez-obexd_5.37-0ubuntu5.3+esm5
- Installed package : libbluetooth3_5.37-0ubuntu5.1
- Fixed package : libbluetooth3_5.37-0ubuntu5.3+esm5

148938 - Ubuntu 16.04 LTS : Dnsmasq vulnerabilities (USN-4924-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4924-1 advisory.

It was discovered that Dnsmasq incorrectly handled certain wildcard synthesized NSEC records. A remote attacker could possibly use this issue to prove the non-existence of hostnames that actually exist.

(CVE-2017-15107)

It was discovered that Dnsmasq incorrectly handled certain large DNS packets. A remote attacker could possibly use this issue to cause Dnsmasq to crash, resulting in a denial of service. (CVE-2019-14513)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4924-1>

Solution

Update the affected dnsmasq, dnsmasq-base and / or dnsmasq-utils 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)

References

CVE	CVE-2017-15107
CVE XREF	CVE-2019-14513 USN:4924-1

Plugin Information

Published: 2021/04/22, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dnsmasq-base 2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.75-1ubuntu0.16.04.10

126947 - Ubuntu 16.04 LTS : Evince vulnerability (USN-4067-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4067-1 advisory.

It was discovered that Evince incorrectly handled certain PDF files. An attacker could possibly use this issue to cause a denial of service 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-4067-1>

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-2019-1010006
XREF USN:4067-1

Plugin Information

Published: 2019/07/23, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : evince_3.18.2-1ubuntu4.3
- Fixed package : evince_3.18.2-1ubuntu4.6
- Installed package : evince-common_3.18.2-1ubuntu4.3
- Fixed package : evince-common_3.18.2-1ubuntu4.6
- Installed package : libevdocument3-4_3.18.2-1ubuntu4.3
- Fixed package : libevdocument3-4_3.18.2-1ubuntu4.6
- Installed package : libevview3-3_3.18.2-1ubuntu4.3
- Fixed package : libevview3-3_3.18.2-1ubuntu4.6

183555 - Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4216-2)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4216-2 advisory.

USN-4216-1 fixed vulnerabilities in Firefox. This update provides the corresponding update for Ubuntu 16.04 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-4216-2>

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-2019-11745
CVE	CVE-2019-11756
CVE	CVE-2019-17005
CVE	CVE-2019-17008
CVE	CVE-2019-17010
CVE	CVE-2019-17011
CVE	CVE-2019-17012
CVE	CVE-2019-17013
CVE	CVE-2019-17014
XREF	IAVA:2019-A-0438-S
XREF	USN:4216-2

Plugin Information

Published: 2023/10/20, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_71.0+build5-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_71.0+build5-0ubuntu0.16.04.1

183716 - Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4278-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4278-2 advisory.

USN-4278-1 fixed vulnerabilities in Firefox. This update provides the corresponding update for Ubuntu 16.04 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-4278-2>

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-2020-6796
CVE	CVE-2020-6798
CVE	CVE-2020-6800
CVE	CVE-2020-6801
XREF	IAVA:2020-A-0072-S
XREF	USN:4278-2

Plugin Information

Published: 2023/10/23, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_73.0.1+build1-0ubuntu0.16.04.1

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_73.0.1+build1-0ubuntu0.16.04.1
```

137178 - Ubuntu 16.04 LTS : FreeRDP vulnerabilities (USN-4382-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4382-1 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-4382-1>

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)

CVSS v3.0 Temporal Score

7.5 (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-2020-11042
CVE	CVE-2020-11045
CVE	CVE-2020-11046
CVE	CVE-2020-11048
CVE	CVE-2020-11049
CVE	CVE-2020-11058
CVE	CVE-2020-11521

CVE	CVE-2020-11522
CVE	CVE-2020-11523
CVE	CVE-2020-11525
CVE	CVE-2020-11526
CVE	CVE-2020-13396
CVE	CVE-2020-13397
CVE	CVE-2020-13398
XREF	USN:4382-1

Plugin Information

Published: 2020/06/05, Modified: 2024/08/29

Plugin Output

tcp/0

```

- Installed package : libfreerdp-cache1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-cache1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-client1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-client1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-codec1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-codec1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-common1.1_0_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-common1.1_0_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-core1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-core1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-crypto1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-crypto1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-gdi1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-gdi1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-locale1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-locale1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-plugins-standard1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-plugins-standard1.1_1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-primitives1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-primitives1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libfreerdp-utils1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libfreerdp-utils1.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-crt0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-crt0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-dsparse0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-dsparse0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-environment0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-environment0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-file0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-file0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-handle0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-handle0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-heap0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-heap0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-input0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-input0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-interlocked0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-interlocked0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-library0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-library0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-path0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-path0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-pool0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-pool0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-registry0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-registry0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-rpc0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-rpc0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-sspi0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-sspi0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

- Installed package : libwinpr-synch0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-synch0.1_1.1_0~git20140921.1.440916e+dfsg1-5ubuntu1.4

```

11/2/25, 1:18 AM

Photographer

- Installed package : libwinpr-sysinfo0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-sysinfo0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4
- Installed package : libwinpr-thread0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-thread0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4
- Installed package : libwinpr-utils0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3
- Fixed package : libwinpr-utils0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4

128630 - Ubuntu 16.04 LTS : FreeType vulnerability (USN-4126-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4126-1 advisory.

It was discovered that FreeType incorrectly handled certain font files. An attacker could possibly use this issue to access 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-4126-1>

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-2015-9383
XREF	USN:4126-1

Plugin Information

Published: 2019/09/10, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libfreetype6_2.6.1-0.1ubuntu2.3
- Fixed package : libfreetype6_2.6.1-0.1ubuntu2.4

123001 - Ubuntu 16.04 LTS : GDK-PixBuf vulnerability (USN-3912-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-3912-1 advisory.

It was discovered that the GDK-PixBuf library did not properly handle certain BMP images. If an user or automated system were tricked into opening a specially crafted BMP 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-3912-1>

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-2017-12447
XREF-USN:3912-1

Plugin Information

Published: 2019/03/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : gir1.2-gdkpixbuf-2.0_2.32.2-1ubuntu1.5
- Fixed package : gir1.2-gdkpixbuf-2.0_2.32.2-1ubuntu1.6

- Installed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.6

- Installed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.6
```

149477 - Ubuntu 16.04 LTS : GNU C Library vulnerabilities (USN-4954-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4954-1 advisory.

Jason Royes and Samuel Dytrych discovered that the `memcpy()` implementation for 32 bit ARM processors in the GNU C Library contained an integer underflow vulnerability. An attacker could possibly use this to cause a denial of service (application crash) or execute arbitrary code. (CVE-2020-6096)

It was discovered that the POSIX regex implementation in the GNU C Library did not properly parse alternatives. An attacker could use this to cause a denial of service. (CVE-2009-5155)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4954-1>

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

7.3 (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-2009-5155
XREF	USN:4954-1

Plugin Information

Published: 2021/05/14, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3

- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3

- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3

- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3

- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3

- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3
```

215239 - Ubuntu 16.04 LTS : GNU C Library vulnerability (USN-7259-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7259-2 advisory.

USN-7259-1 fixed a vulnerability in GNU C Library. This update provides the corresponding update for Ubuntu 16.04 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-7259-2>

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:7259-2

Plugin Information

Published: 2025/02/10, Modified: 2025/02/10

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 : libc-bin_2.23-0ubuntu11
- Fixed package : libc-bin_2.23-0ubuntu11.3+esm8
- Installed package : libc-dev-bin_2.23-0ubuntu11
- Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm8
- Installed package : libc6_2.23-0ubuntu11
- Fixed package : libc6_2.23-0ubuntu11.3+esm8
- Installed package : libc6-dev_2.23-0ubuntu11
- Fixed package : libc6-dev_2.23-0ubuntu11.3+esm8
- Installed package : locales_2.23-0ubuntu11
- Fixed package : locales_2.23-0ubuntu11.3+esm8
- Installed package : multiarch-support_2.23-0ubuntu11
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm8

144849 - Ubuntu 16.04 LTS : JasPer vulnerabilities (USN-4688-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4688-1 advisory.

It was discovered that Jasper incorrectly certain files. An attacker could possibly use this issue to cause a crash. (CVE-2018-18873)

It was discovered that Jasper incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-19542)

It was discovered that Jasper incorrectly handled certain JPC encoders. An attacker could possibly use this issue to execute arbitrary code. (CVE-2020-27828)

11/2/25, 1:18 AM

Photographer

It was discovered that Jasper incorrectly handled certain images. An attacker could possibly use this issue to expose sensitive information or cause a crash. (CVE-2017-9782)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4688-1>

Solution

Update the affected libjasper-dev, libjasper-runtime and / or libjasper1 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

BID	107792
CVE	CVE-2017-9782
CVE	CVE-2018-18873
CVE	CVE-2018-19542
CVE	CVE-2020-27828
XREF	USN:4688-1

Plugin Information

Published: 2021/01/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libjasper1_1.900.1-debian1-2.4ubuntu1.2
- Fixed package : libjasper1_1.900.1-debian1-2.4ubuntu1.3
```

133351 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4255-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4255-2 advisory.

USN-4255-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 LTS for Ubuntu 16.04 LTS.

It was discovered that the Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors. A local attacker could use this to expose sensitive information.

(CVE-2019-14615)

It was discovered that a race condition can lead to a use-after-free while destroying GEM contexts in the i915 driver for the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2020-7053)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4255-2>

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-2019-14615
CVE	CVE-2020-7053
XREF	USN:4255-2

Plugin Information

Published: 2020/01/30, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-76-generic for this advisory.

207279 - Ubuntu 16.04 LTS : OpenSSH vulnerability (USN-6560-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6560-3 advisory.

USN-6560-2 fixed a vulnerability in OpenSSH. This update provides the corresponding update for Ubuntu 16.04 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-6560-3>

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

I

References

CVE	CVE-2023-51385
XREF	IAVA:2023-A-0701-S
XREF	USN:6560-3

Plugin Information

Published: 2024/09/16, Modified: 2024/09/16

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.

- Installed package : openssh-client_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-client_1:7.2p2-4ubuntu2.10+esm6
- Installed package : openssh-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-server_1:7.2p2-4ubuntu2.10+esm6
- Installed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm6

216330 - Ubuntu 16.04 LTS : libsndfile vulnerability (USN-7267-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7267-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-7267-1>

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs 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-2024-50612
XREF	USN:7267-1

Plugin Information

Published: 2025/02/14, Modified: 2025/02/14

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 : libsndfile1_1.0.25-10ubuntu0.16.04.1
- Fixed package : libsndfile1_1.0.25-10ubuntu0.16.04.3+esm4

10114 - ICMP Timestamp Request Remote Date Disclosure**Synopsis**

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The remote clock is synchronized with the local clock.

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/VC:N/V:I:N/V:A: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

Plugin Information

Published: 2025/04/07, Modified: 2025/04/17

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm27

- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm27

- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm27

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm27
```

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/U: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

IAVA:2024-A-0618-S

Plugin Information

Published: 2024/11/27, Modified: 2025/08/19

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.

- Installed package : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm26
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm26
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm26
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm26

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-2023-39804
XREF USN:6543-1

Plugin Information

Published: 2023/12/11, Modified: 2024/11/13

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.

- Installed package : tar_1.28-2.1ubuntu0.1
- Fixed package : tar_1.28-2.1ubuntu0.2+esm3

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

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 : libprocps4_2:3.3.10-4ubuntu2.4
- Fixed package : libprocps4_2:3.3.10-4ubuntu2.5+esm1
- Installed package : procps_2:3.3.10-4ubuntu2.4
- Fixed package : procps_2:3.3.10-4ubuntu2.5+esm1

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.

Danil 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 XREF [CVE-2023-20569](#) [USN:6319-1](#)

Plugin Information

Published: 2023/08/30, 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.

- Installed package : `amd64-microcode_3.20180524.1~ubuntu0.16.04.2`
- Fixed package : `amd64-microcode_3.20191021.1+really3.20180524.1~ubuntu0.16.04.2+esm2`

182932 - Ubuntu 16.04 ESM / 18.04 ESM : curl vulnerability (USN-6429-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6429-2 advisory.

USN-6429-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 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-6429-2>

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:L/A:N)

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:P/A:N)

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE-XREF	CVE-2023-38546 USN:6429-2
XREF	CEA-ID:CEA-2023-0052
XREF	IAVA:2023-A-0531-S

Plugin Information

Published: 2023/10/11, Modified: 2024/10/30

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm10
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm10

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
XREF	CVE-2021-0561

Plugin Information

Published: 2022/11/21, Modified: 2024/08/29

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 : libflac8_1.3.1-4
- Fixed package : libflac8_1.3.1-4ubuntu0.1~esm1

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

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 : krb5-locales_1.13.2+dfsg-5ubuntu2.1
- Fixed package : krb5-locales_1.13.2+dfsg-5ubuntu2.2+esm3
- Installed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libgssapi-krb5-2_1.13.2+dfsg-5ubuntu2.2+esm3
- Installed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libk5crypto3_1.13.2+dfsg-5ubuntu2.2+esm3
- Installed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5-3_1.13.2+dfsg-5ubuntu2.2+esm3
- Installed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.1
- Fixed package : libkrb5support0_1.13.2+dfsg-5ubuntu2.2+esm3

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
XREF	CVE-2022-21166 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-187-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

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm5
- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm5

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

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 : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm2
- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm2

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
-----	--------------------------------

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-188-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
XREF

CVE-2021-3008/
USN:5391-1

Plugin Information

Published: 2022/04/27, 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.

- Installed package : libsepol1_2.4-2
- Fixed package : libsepol1_2.4-2ubuntu0.1~esm1

158728 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5319-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5319-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5319-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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-2022-0001
CVE	CVE-2022-0002
XREF	USN:5319-1

Plugin Information

Published: 2022/03/09, Modified: 2024/08/29

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.

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-171-generic for this advisory.

155655 - Ubuntu 16.04 ESM / 18.04 LTS : OpenEXR vulnerability (USN-5150-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5150-1 advisory.

It was discovered that OpenEXR incorrectly handled certain EXR image files. 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-5150-1>

Solution

Update the affected libopenexr-dev, libopenexr22 and / or openexr packages.

Risk Factor

Low

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/R:L/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-2021-3941
XREF	USN:5150-1

Plugin Information

Published: 2021/11/20, 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.

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.6+esm3

168208 - Ubuntu 16.04 ESM / 18.04 LTS : libICE vulnerability (USN-5744-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5744-1 advisory.

It was discovered that libICE was using a weak mechanism to generate the session cookies. A local attacker could possibly use this issue to perform a privilege escalation 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-5744-1>

Solution

Update the affected libice-dev and / or libice6 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-2017-2626
XREF-USN:5744-1

Plugin Information

Published: 2022/11/28, 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.

- Installed package : libice6_2:1.0.9-1
- Fixed package : libice6_2:1.0.9-1ubuntu0.16.04.1+esm1

152918 - Ubuntu 16.04 ESM : APR vulnerability (USN-5056-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5056-1 advisory.

It was discovered that APR 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-5056-1>

Solution

Update the affected libapr1 and / or libapr1-dev 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:H/I:N/A:H)

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:N/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE XREF [CVE-2021-35940](#)
USN:5056-1

Plugin Information

Published: 2021/08/31, 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.

- Installed package : libapr1_1.5.2-3
- Fixed package : libapr1_1.5.2-3ubuntu0.1~esm1

168150 - Ubuntu 16.04 ESM : APR-util vulnerability (USN-5737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5737-1 advisory.

It was discovered that APR-util did not properly handle memory when using

SDBM database files. A local attacker with write access to the database

can make a program or process using these functions crash, and 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-5737-1>

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

1.9 (CVSS2#AV:L/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-12618
XREF	USN:5737-1

Plugin Information

Published: 2022/11/23, Modified: 2025/02/20

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 : libaprutil1_1.5.4-1build1
- Fixed package : libaprutil1_1.5.4-1ubuntu0.1~esm1
- Installed package : libaprutil1-dbd-sqlite3_1.5.4-1build1
- Fixed package : libaprutil1-dbd-sqlite3_1.5.4-1ubuntu0.1~esm1
- Installed package : libaprutil1-ldap_1.5.4-1build1
- Fixed package : libaprutil1-ldap_1.5.4-1ubuntu0.1~esm1

149908 - Ubuntu 16.04 ESM : Apport vulnerabilities (USN-4965-2)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4965-2 advisory.

USN-4965-1 fixed several vulnerabilities in Apport. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4965-2>

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:4965-2

Plugin Information

Published: 2021/05/25, Modified: 2024/10/29

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 : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30+esm1
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30+esm1
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30+esm1
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30+esm1

151451 - Ubuntu 16.04 ESM : Avahi vulnerability (USN-5008-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5008-2 advisory.

USN-5008-1 fixed a vulnerability in avahi. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5008-2>

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

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2021-3468

XREF USN:5008-2

Plugin Information

Published: 2021/07/08, Modified: 2024/10/29

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 : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-client3_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common-data_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-common3_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-glib1_0.6.32~rc+dfsg-1ubuntu2.3+esm1
- Installed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3
- Fixed package : libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3+esm1

150028 - Ubuntu 16.04 ESM : DHCP vulnerability (USN-4969-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-4969-2 advisory.

USN-4969-1 fixed a vulnerability in DHCP. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4969-2>

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:4969-2

Plugin Information

Published: 2021/05/27, Modified: 2024/10/29

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 : `isc-dhcp-client_4.3.3-5ubuntu12.10`
- Fixed package : `isc-dhcp-client_4.3.3-5ubuntu12.10+esm1`
- Installed package : `isc-dhcp-common_4.3.3-5ubuntu12.10`
- Fixed package : `isc-dhcp-common_4.3.3-5ubuntu12.10+esm1`

168518 - Ubuntu 16.04 ESM : GCC vulnerability (USN-5770-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5770-1 advisory.

Todd Eisenberger discovered that certain versions of GNU Compiler Collection (GCC) could be made to clobber the status flag of RDRAND and RDSEED with specially crafted input. This could potentially lead to less randomness in random number generation.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5770-1>

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:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE XREF	CVE-2017-11671 USN:5770-1
-------------	--

Plugin Information

Published: 2022/12/08, Modified: 2024/08/29

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 : cpp-5_5.4.0-6ubuntu1~16.04.11
- Fixed package : cpp-5_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : g++-5_5.4.0-6ubuntu1~16.04.11
- Fixed package : g++-5_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : gcc-5_5.4.0-6ubuntu1~16.04.11
- Fixed package : gcc-5_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : gcc-5-base_5.4.0-6ubuntu1~16.04.11
- Fixed package : gcc-5-base_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : gcc-6-base_6.0.1-0ubuntu1
- Fixed package : gcc-6-base_6.0.1-0ubuntu1+esm1
- Installed package : libasan2_5.4.0-6ubuntu1~16.04.11
- Fixed package : libasan2_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libatomic1_5.4.0-6ubuntu1~16.04.11
- Fixed package : libatomic1_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libcc1-0_5.4.0-6ubuntu1~16.04.11
- Fixed package : libcc1-0_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libcilkkrts5_5.4.0-6ubuntu1~16.04.11
- Fixed package : libcilkkrts5_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libgcc-5-dev_5.4.0-6ubuntu1~16.04.11
- Fixed package : libgcc-5-dev_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libgcc1_1:6.0.1-0ubuntu1
- Fixed package : libgcc1_1:6.0.1-0ubuntu1+esm1
- Installed package : libgomp1_5.4.0-6ubuntu1~16.04.11
- Fixed package : libgomp1_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libitm1_5.4.0-6ubuntu1~16.04.11
- Fixed package : libitm1_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : liblsan0_5.4.0-6ubuntu1~16.04.11
- Fixed package : liblsan0_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libmpx0_5.4.0-6ubuntu1~16.04.11
- Fixed package : libmpx0_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libquadmath0_5.4.0-6ubuntu1~16.04.11
- Fixed package : libquadmath0_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libstdc++-5-dev_5.4.0-6ubuntu1~16.04.11
- Fixed package : libstdc++-5-dev_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libstdc++6_5.4.0-6ubuntu1~16.04.11
- Fixed package : libstdc++6_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libtsan0_5.4.0-6ubuntu1~16.04.11
- Fixed package : libtsan0_5.4.0-6ubuntu1~16.04.12+esm2
- Installed package : libubsan0_5.4.0-6ubuntu1~16.04.11
- Fixed package : libubsan0_5.4.0-6ubuntu1~16.04.12+esm2

171812 - Ubuntu 16.04 ESM : Linux kernel (HWE) vulnerabilities (USN-5883-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5883-1 advisory.

Kyle Zeng discovered that the sysctl implementation in the Linux kernel contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-4378)

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)

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)

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)

Johannes Wikner and Kaveh Razavi discovered that for some AMD x86-64 processors, the branch predictor could be mis-trained for return instructions in certain circumstances. A local attacker could possibly use this to expose sensitive information. (CVE-2022-29900)

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)

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 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)

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)

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)

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 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)

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)

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 USB monitoring (usbmon) component in the Linux kernel did not properly set permissions on memory mapped 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)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5883-1>

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

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-2022-2663
CVE	CVE-2022-3521
CVE	CVE-2022-3545
CVE	CVE-2022-3628
CVE	CVE-2022-3640
CVE	CVE-2022-3646
CVE	CVE-2022-3649
CVE	CVE-2022-4378
CVE	CVE-2022-20369
CVE	CVE-2022-26373
CVE	CVE-2022-29900
CVE	CVE-2022-29901
CVE	CVE-2022-39842
CVE	CVE-2022-41849
CVE	CVE-2022-41850
CVE	CVE-2022-42328
CVE	CVE-2022-42895
CVE	CVE-2022-43750
CVE	CVE-2023-0461
XREF	USN:5883-1

Plugin Information

Published: 2023/02/22, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-206-generic for this advisory.

166006 - Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5669-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5669-2 advisory.

It was discovered that the SUNRPC RDMA protocol implementation in the Linux kernel did not properly calculate the header size of a RPC message payload. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-0812)

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)

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)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5669-2>

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

7.1 (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-2022-0812
CVE	CVE-2022-1012
CVE	CVE-2022-2318
CVE	CVE-2022-26365
CVE	CVE-2022-32296
CVE	CVE-2022-33740
CVE	CVE-2022-33741
CVE	CVE-2022-33742
CVE	CVE-2022-33744
XREF	USN:5669-2

Plugin Information

Published: 2022/10/11, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-194-generic for this advisory.

160507 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5400-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5400-2 advisory.

USN-5400-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5400-2>

Solution

Update the affected packages.

Risk Factor

Low

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

2.1 (CVSS:2.0/AV:N/AC:H/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS:2.0/E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-21417
CVE	CVE-2022-21427
CVE	CVE-2022-21444
CVE	CVE-2022-21451
CVE	CVE-2022-21454
CVE	CVE-2022-21460
XREF	USN:5400-2
XREF	IAVA:2022-A-0168-S

Plugin Information

Published: 2022/05/04, Modified: 2024/10/29

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 : libmysqlclient20_5.7.30-0ubuntu0.16.04.1
- Fixed package : libmysqlclient20_5.7.38-0ubuntu0.16.04.1+esm1
- Installed package : mysql-common_5.7.30-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.38-0ubuntu0.16.04.1+esm1

157372 - Ubuntu 16.04 ESM : Perl DBI module vulnerabilities (USN-5030-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

11/2/25, 1:18 AM

Photographer

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5030-2 advisory.

USN-5030-1 addressed vulnerabilities in Perl DBI module. This

update provides the corresponding updates for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5030-2>

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_XREF	CVE-2020-14393 USN-5030-2

Plugin Information

Published: 2022/02/04, Modified: 2024/10/29

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 : libdbi-perl_1.634-1build1
- Fixed package : libdbi-perl_1.634-1ubuntu0.2+esm1

162471 - Ubuntu 16.04 ESM : Protocol Buffers vulnerability (USN-5490-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5490-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5490-1>

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

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:O/RC:C)

References

CVE	CVE-2021-22570
XREF	USN:5490-1

Plugin Information

Published: 2022/06/22, 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.

- Installed package : libprotobuf-lite9v5_2.6.1-1.3
- Fixed package : libprotobuf-lite9v5_2.6.1-1.3ubuntu0.1~esm1
- Installed package : libprotobuf9v5_2.6.1-1.3
- Fixed package : libprotobuf9v5_2.6.1-1.3ubuntu0.1~esm1

166261 - Ubuntu 16.04 ESM : libXdmcp vulnerability (USN-5690-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5690-1 advisory.

It was discovered that libXdmcp was generating weak session keys. A local attacker could possibly use this issue to perform a brute force attack and obtain another user's key.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5690-1>

Solution

Update the affected libxdmcp-dev and / or libxdmcp6 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-2017-2625
XREF	USN:5690-1

Plugin Information

Published: 2022/10/19, 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.

- Installed package : libxdmcp6_1:1.1.2-1.1
- Fixed package : libxdmcp6_1:1.1.2-1.1ubuntu0.1~esm1

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:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2025-5054
XREF	USN:7545-1

Plugin Information

Published: 2025/06/03, Modified: 2025/06/03

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 : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30+esm5
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30+esm5
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30+esm5
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30+esm5

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 Flenkas 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_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript_9.26~dfsg+0~0ubuntu0.16.04.14+esm9`
- Installed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `ghostscript-x_9.26~dfsg+0~0ubuntu0.16.04.14+esm9`
- Installed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9_9.26~dfsg+0~0ubuntu0.16.04.14+esm9`
- Installed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.7`
- Fixed package : `libgs9-common_9.26~dfsg+0~0ubuntu0.16.04.14+esm9`

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

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 : `libraw15_0.17.1-1ubuntu0.4`
- Fixed package : `libraw15_0.17.1-1ubuntu0.5+esm1`

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	CVE-2024-56378
XREF	USN:7213-1

Plugin Information

Published: 2025/01/17, Modified: 2025/01/17

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 : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16+esm5
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16+esm5
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16+esm5

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_2.32.2-1ubuntu1.5
- Fixed package : gir1.2-gdkpixbuf-2.0_2.32.2-1ubuntu1.6+esm2
- Installed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-0_2.32.2-1ubuntu1.6+esm2
- Installed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.5
- Fixed package : libgdk-pixbuf2.0-common_2.32.2-1ubuntu1.6+esm2

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/V/A: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: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

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 : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20240910.0ubuntu0.16.04.1+esm1

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:OF/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

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 : vim_2:7.4.1689-3ubuntu1.4
- Fixed package : vim_2:7.4.1689-3ubuntu1.5+esm25
- Installed package : vim-common_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm25
- Installed package : vim-runtime_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-runtime_2:7.4.1689-3ubuntu1.5+esm25
- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.4
- Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm25

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
XREF	USN:4664-1

Plugin Information

Published: 2020/12/09, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : aptdaemon_1.1.1+bzr982-0ubuntu14
- Fixed package : aptdaemon_1.1.1+bzr982-0ubuntu14.5

- Installed package : aptdaemon-data_1.1.1+bzr982-0ubuntu14
- Fixed package : aptdaemon-data_1.1.1+bzr982-0ubuntu14.5

- Installed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu14.5

- Installed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu14.5

- Installed package : python3-aptdaemon.pkcompat_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon.pkcompat_1.1.1+bzr982-0ubuntu14.5
```

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+bzr982-0ubuntu14
- Fixed package : aptdaemon_1.1.1+bzr982-0ubuntu14.4
- Installed package : aptdaemon-data_1.1.1+bzr982-0ubuntu14
- Fixed package : aptdaemon-data_1.1.1+bzr982-0ubuntu14.4
- Installed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon_1.1.1+bzr982-0ubuntu14.4
- Installed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon.gtk3widgets_1.1.1+bzr982-0ubuntu14.4
- Installed package : python3-aptdaemon.pkcompat_1.1.1+bzr982-0ubuntu14
- Fixed package : python3-aptdaemon.pkcompat_1.1.1+bzr982-0ubuntu14.4

[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
-----	--------------------------------

Plugin Information

Published: 2021/04/26, Modified: 2024/08/28

Plugin Output

tcp/0

```
- Installed package : file-roller_3.16.5-0ubuntu1.2
- Fixed package : file-roller_3.16.5-0ubuntu1.5
```

137352 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode regression (USN-4385-2)

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-4385-2 advisory.

USN-4385-1 provided updated Intel Processor Microcode. Unfortunately, that update prevented certain processors in the Intel Skylake family (06_4EH) from booting successfully. Additionally, on Ubuntu 20.04 LTS, late loading of microcode was enabled, which could lead to system instability. This update reverts the microcode update for the Skylake processor family and disables the late loading option on Ubuntu 20.04 LTS.

Please note that the 'dis_uicode_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-4385-2>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

References

XREF USN:4385-2

Plugin Information

Published: 2020/06/11, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20200609.0ubuntu0.16.04.1
```

137295 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4385-1)

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-4385-1 advisory.

It was discovered that memory contents previously stored in microarchitectural special registers after RDRAND, RDSEED, and SGX EGETKEY read operations on Intel client and Xeon E3 processors may be briefly exposed to processes on the same or different processor cores. A local attacker could use this to expose sensitive information. (CVE-2020-0543)

It was discovered that on some Intel processors, partial data values previously read from a vector register on a physical core may be propagated into unused portions of the store buffer. A local attacker could possibly use this to expose sensitive information. (CVE-2020-0548)

It was discovered that on some Intel processors, data from the most recently evicted modified L1 data cache (L1D) line may be propagated into an unused (invalid) L1D fill buffer. A local attacker could possibly use this to expose sensitive information. (CVE-2020-0549)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4385-1>

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-2020-0543
CVE	CVE-2020-0548
CVE	CVE-2020-0549
XREF	USN:4385-1

Plugin Information

Published: 2020/06/10, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20200609.0ubuntu0.16.04.0

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_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20201110.0ubuntu0.16.04.1

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-XREF CVE-2020-8694
USN:4627-1

Plugin Information

Published: 2020/11/11, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-123-generic for this advisory.

138167 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-4417-1)**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-4417-1 advisory.

Cesar Pereida, Billy Bob Brumley, Yuval Yarom, and Nicola Tuveri discovered that NSS incorrectly handled RSA key generation. A local attacker could possibly use this issue to perform a timing attack and recover RSA 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-4417-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.4 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/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

CVSS v2.0 Temporal Score

0.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-12402
XREF	USN:4417-1

Plugin Information

Published: 2020/07/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libnss3_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3_2:3.28.4-0ubuntu0.16.04.12
- Installed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.4
- Fixed package : libnss3-nssdb_2:3.28.4-0ubuntu0.16.04.12

138168 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4418-1)

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-4418-1 advisory.

It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image 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-4418-1>

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

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-2020-15305
CVE	CVE-2020-15306
XREF	USN:4418-1

Plugin Information

Published: 2020/07/07, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libopenexr22_2.2.0-10ubuntu2
- Fixed package : libopenexr22_2.2.0-10ubuntu2.3

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
XREF	CVE-2020-16122
	USN:4538-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : gir1.2-packagekitglib-1.0_0.8.17-4ubuntu6~gcc5.4ubuntu1.4
- Fixed package : gir1.2-packagekitglib-1.0_0.8.17-4ubuntu6~gcc5.4ubuntu1.5
- Installed package : libpackagekit-glib2-16_0.8.17-4ubuntu6~gcc5.4ubuntu1.4
- Fixed package : libpackagekit-glib2-16_0.8.17-4ubuntu6~gcc5.4ubuntu1.5

136546 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : PulseAudio vulnerability (USN-4355-1)

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-4355-1 advisory.

PulseAudio in Ubuntu contains additional functionality to mediate audio recording for snap packages and it was discovered that this functionality did not mediate PulseAudio module unloading. An attacker-controlled snap with only the audio-playback interface connected could exploit this to bypass access controls and record audio.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4355-1>

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

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-2020-11931
XREF	USN:4355-1

Plugin Information

Published: 2020/05/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.10
- Fixed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.12
- Installed package : libpulse0_1:8.0-0ubuntu3.10
- Fixed package : libpulse0_1:8.0-0ubuntu3.12
- Installed package : libpulsedsp_1:8.0-0ubuntu3.10
- Fixed package : libpulsedsp_1:8.0-0ubuntu3.12
- Installed package : pulseaudio_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio_1:8.0-0ubuntu3.12
- Installed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.12
- Installed package : pulseaudio-module-x11_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-x11_1:8.0-0ubuntu3.12
- Installed package : pulseaudio-utils_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-utils_1:8.0-0ubuntu3.12

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 [CVE-2020-16123](#)

XREF [USN:4640-1](#)

Plugin Information

Published: 2020/11/24, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.10
- Fixed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.15

- Installed package : libpulse0_1:8.0-0ubuntu3.10
- Fixed package : libpulse0_1:8.0-0ubuntu3.15

- Installed package : libpulsedsp_1:8.0-0ubuntu3.10
- Fixed package : libpulsedsp_1:8.0-0ubuntu3.15

- Installed package : pulseaudio_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio_1:8.0-0ubuntu3.15

- Installed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.15

- Installed package : pulseaudio-module-x11_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-x11_1:8.0-0ubuntu3.15

- Installed package : pulseaudio-utils_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-utils_1:8.0-0ubuntu3.15
```

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_0.96.20.9
- Fixed package : python3-software-properties_0.96.20.10
- Installed package : software-properties-common_0.96.20.9
- Fixed package : software-properties-common_0.96.20.10
- Installed package : software-properties-gtk_0.96.20.9
- Fixed package : software-properties-gtk_0.96.20.10

137553 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : fwupd vulnerability (USN-4395-1)**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-4395-1 advisory.

Justin Steven discovered that fwupd incorrectly handled certain signature verification. An attacker could possibly use this issue to install an unsigned firmware.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4395-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

6.0 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:P/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

2.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-10759
XREF	USN:4395-1

Plugin Information

Published: 2020/06/17, Modified: 2024/08/29

Plugin Output

tcp/0

- Installed package : fwupd_0.8.3-0ubuntu4
- Fixed package : fwupd_0.8.3-0ubuntu5.1
- Installed package : libdfu1_0.8.3-0ubuntu4
- Fixed package : libdfu1_0.8.3-0ubuntu5.1
- Installed package : libfwupd1_0.8.3-0ubuntu4
- Fixed package : libfwupd1_0.8.3-0ubuntu5.1

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:OF/RC:C)

References

CVE
XREF

CVE-2020-15704

USN:4451-1

Plugin Information

Published: 2020/08/06, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : ppp_2.4.7-1+2ubuntu1.16.04.1
- Fixed package : ppp_2.4.7-1+2ubuntu1.16.04.3

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_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python-apt-common_1.1.0~beta1ubuntu0.16.04.10
- Installed package : python3-apt_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python3-apt_1.1.0~beta1ubuntu0.16.04.10

135171 - Ubuntu 16.04 LTS / 18.04 LTS : Apport vulnerabilities (USN-4315-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4315-1 advisory.

Maximilien Bourgeteau discovered that the Apport lock file was created with insecure permissions. This could allow a local attacker to escalate their privileges via a symlink attack. (CVE-2020-8831)

Maximilien Bourgeteau discovered a race condition in Apport when setting crash report permissions. This could allow a local attacker to read arbitrary files via a symlink attack.

(CVE-2020-8833)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4315-1>

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

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:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-8831
CVE	CVE-2020-8833
XREF	USN:4315-1

Plugin Information

Published: 2020/04/02, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.23
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.23
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.23
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.23

125852 - Ubuntu 16.04 LTS / 18.04 LTS : DBus vulnerability (USN-4015-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4015-1 advisory.

Joe Vennix discovered that DBus incorrectly handled DBUS_COOKIE_SHA1 authentication. A local attacker could possibly use this issue to bypass authentication and connect to DBus servers with elevated 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-4015-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:L/AC:L/PR:L/U: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:O/RC:C)

References

CVE	CVE-2019-12749
XREF	USN:4015-1

Plugin Information

Published: 2019/06/12, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : dbus_1.10.6-1ubuntu3.3
- Fixed package : dbus_1.10.6-1ubuntu3.4
- Installed package : dbus-x11_1.10.6-1ubuntu3.3
- Fixed package : dbus-x11_1.10.6-1ubuntu3.4
- Installed package : libdbus-1-3_1.10.6-1ubuntu3.3
- Fixed package : libdbus-1-3_1.10.6-1ubuntu3.4

129384 - Ubuntu 16.04 LTS / 18.04 LTS : File Roller vulnerability (USN-4139-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4139-1 advisory.

It was discovered that File Roller incorrectly handled certain TAR files. An attacker could possibly use this issue to overwrite sensitive files during extraction.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4139-1>

Solution

Update the affected file-roller package.

Risk Factor

Low

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

3.9 (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:P/A:N)

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-16680
XREF	USN:4139-1

Plugin Information

Published: 2019/09/26, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : file-roller_3.16.5-0ubuntu1.2
- Fixed package : file-roller_3.16.5-0ubuntu1.3

135847 - Ubuntu 16.04 LTS / 18.04 LTS : File Roller vulnerability (USN-4332-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4332-1 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-4332-1>

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

3.4 (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-2020-11736
XREF	USN:4332-1

Plugin Information

Published: 2020/04/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : file-roller_3.16.5-0ubuntu1.2
- Fixed package : file-roller_3.16.5-0ubuntu1.4
```

128967 - Ubuntu 16.04 LTS / 18.04 LTS : IBus vulnerability (USN-4134-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4134-1 advisory.

Simon McVittie discovered that IBus did not enforce appropriate access controls on its private D-Bus socket. A local unprivileged user who discovers the IBus socket address of another user could exploit this to capture the key strokes of the other 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-4134-1>

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: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	CVE-2019-14822
XREF	USN:4134-1

Plugin Information

Published: 2019/09/17, Modified: 2024/08/28

Plugin Output

tcp/0

- Installed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.1
- Fixed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.2
- Installed package : ibus_1.5.11-1ubuntu2.1
- Fixed package : ibus_1.5.11-1ubuntu2.2
- Installed package : ibus-gtk_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk_1.5.11-1ubuntu2.2
- Installed package : ibus-gtk3_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk3_1.5.11-1ubuntu2.2
- Installed package : libibus-1.0-5_1.5.11-1ubuntu2.1
- Fixed package : libibus-1.0-5_1.5.11-1ubuntu2.2

134888 - Ubuntu 16.04 LTS / 18.04 LTS : IBus vulnerability (USN-4134-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4134-3 advisory.

USN-4134-1 fixed a vulnerability in IBus. The update caused a regression in some Qt applications and the fix was subsequently reverted in USN-4134-2. The regression has since been resolved and so this update fixes the original vulnerability.

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-4134-3>

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:H/I:H/A:N)

CVSS v3.0 Temporal Score

6.2 (CVSS:3.0/E:U/R:L/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	CVE-2019-14822
XREF	USN:4134-3

Plugin Information

Published: 2020/03/25, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.1
- Fixed package : gir1.2-ibus-1.0_1.5.11-1ubuntu2.4
- Installed package : ibus_1.5.11-1ubuntu2.1
- Fixed package : ibus_1.5.11-1ubuntu2.4
- Installed package : ibus-gtk_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk_1.5.11-1ubuntu2.4
- Installed package : ibus-gtk3_1.5.11-1ubuntu2.1
- Fixed package : ibus-gtk3_1.5.11-1ubuntu2.4
- Installed package : libibus-1.0-5_1.5.11-1ubuntu2.1
- Fixed package : libibus-1.0-5_1.5.11-1ubuntu2.4

131694 - Ubuntu 16.04 LTS / 18.04 LTS : Intel Microcode regression (USN-4182-3)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4182-3 advisory.

USN-4182-1 provided updated Intel Processor Microcode. A regression was discovered that caused some Skylake processors to hang after a warm reboot. This update reverts the microcode for that specific processor family.

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-4182-3>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

References

XREF USN:4182-3

Plugin Information

Published: 2019/12/04, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20191115.1ubuntu0.16.04.2

130962 - Ubuntu 16.04 LTS / 18.04 LTS : Intel Microcode update (USN-4182-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4182-1 advisory.

Stephan van Schaik, Alyssa Milburn, Sebastian sterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Giorgi Maisuradze, Moritz Lipp, Michael Schwarz, Daniel Grüss, and Jo Van Bulck discovered that Intel processors using Transactional Synchronization Extensions (TSX) could expose memory contents previously stored in microarchitectural buffers to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11135)

It was discovered that certain Intel Xeon processors did not properly restrict access to a voltage modulation interface. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2019-11139)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4182-1>

Solution

Update the affected intel-microcode package.

Risk Factor

Low

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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-2019-11135

CVE CVE-2019-11139

XREF USN:4182-3

Plugin Information

Published: 2019/11/13, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : intel-microcode_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20191112-0ubuntu0.16.04.2

134660 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4302-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4302-1 advisory.

Paulo Bonzini discovered that the KVM hypervisor implementation in the Linux kernel could improperly let a nested (level 2) guest access the resources of a parent (level 1) guest in certain situations. An attacker could use this to expose sensitive information. (CVE-2020-2732)

Gregory Herrero discovered that the fix for CVE-2019-14615 to address the Linux kernel not properly clearing data structures on context switches for certain Intel graphics processors was incomplete. A local attacker could use this to expose sensitive information. (CVE-2020-8832)

It was discovered that the IPMI message handler implementation in the Linux kernel did not properly deallocate memory in certain situations. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19046)

It was discovered that the Intel WiMAX 2400 driver in the Linux kernel did not properly deallocate memory in certain situations. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19051)

It was discovered that the Marvell Wi-Fi device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could use this to possibly cause a denial of service (kernel memory exhaustion). (CVE-2019-19056)

It was discovered that the Intel(R) Wi-Fi device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19058)

It was discovered that the Brocade BFA Fibre Channel device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19066)

It was discovered that the Realtek RTL8xxx USB Wi-Fi device driver in the Linux kernel did not properly deallocate memory in certain error conditions. A local attacker could possibly use this to cause a denial of service (kernel memory exhaustion). (CVE-2019-19068)

It was discovered that ZR364XX Camera USB device driver for the Linux kernel did not properly initialize memory. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2019-15217)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4302-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.1 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

2.3 (CVSS2#AV:A/AC:M/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-15217
CVE	CVE-2019-19046
CVE	CVE-2019-19051
CVE	CVE-2019-19056
CVE	CVE-2019-19058
CVE	CVE-2019-19066
CVE	CVE-2019-19068
CVE	CVE-2020-2732
CVE	CVE-2020-8832
XREF	USN:4302-1

Plugin Information

Published: 2020/03/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-91-generic for this advisory.
```

135269 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4318-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4318-1 advisory.

Al Viro discovered that the vfs layer 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 expose sensitive information (kernel memory). (CVE-2020-8428)

Gustavo Romero and Paul Mackerras discovered that the KVM implementation in the Linux kernel for PowerPC processors did not properly keep guest state separate from host state. A local attacker in a KVM guest could use this to cause a denial of service (host system crash). (CVE-2020-8834)

Shijie Luo discovered that the ext4 file system implementation in the Linux kernel did not properly check for a too-large journal size. An attacker could use this to construct a malicious ext4 image that, when mounted, could cause a denial of service (soft lockup). (CVE-2020-8992)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4318-1>

Solution

Update the affected kernel 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:N/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:P/I:N/A:P)

CVSS v2.0 Temporal Score

2.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-8428
CVE	CVE-2020-8834

CVE
XREF

CVE-2020-27170
USN:4318-1

Plugin Information

Published: 2020/04/07, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-96-generic for this advisory.

148108 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4890-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4890-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4890-1>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

6.0 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/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

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-2020-27170
CVE	CVE-2020-27171
XREF	USN:4890-1

Plugin Information

Published: 2021/03/25, Modified: 2024/08/27

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-140-generic for this advisory.

140646 - Ubuntu 16.04 LTS / 18.04 LTS : Perl DBI module vulnerability (USN-4503-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4503-1 advisory.

It was discovered that Perl DBI module incorrectly handled certain calls. 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-4503-1>

Solution

Update the affected libdbi-perl 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-2020-14392
XREF USN:4503-1

Plugin Information

Published: 2020/09/17, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libdbi-perl_1.634-1build1
- Fixed package : libdbi-perl_1.634-1ubuntu0.1

140752 - Ubuntu 16.04 LTS / 18.04 LTS : Perl DBI module vulnerability (USN-4534-1)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4534-1 advisory.

It was discovered that Perl DBI module incorrectly handled certain inputs. An attacker could possibly use this issue to cause a 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-4534-1>

Solution

Update the affected libdbi-perl 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: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

1.9 (CVSS2#AV:L/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE
XREF [CVE-2019-20919](#)
 USN:4534-1

Plugin Information

Published: 2020/09/23, Modified: 2024/08/27

Plugin Output

tcp/0

- Installed package : libdbi-perl 1.634-1build1
- Fixed package : libdbi-perl_1.634-1ubuntu0.2

133206 - Ubuntu 16.04 LTS / 18.04 LTS : python-apt regression (USN-4247-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4247-2 advisory.

USN-4247-1 fixed vulnerabilities in python-apt. The updated packages caused a regression when attempting to upgrade to a new Ubuntu release. 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-4247-2>

Solution

Update the affected packages.

Risk Factor

Low

References

XREF USN:4247-2

Plugin Information

Published: 2020/01/23, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : python-apt-common_1.1.0~beta1ubuntu0.16.04.2
- Fixed package   : python-apt-common_1.1.0~beta1ubuntu0.16.04.8

- Installed package : python3-apt_1.1.0~beta1ubuntu0.16.04.2
- Fixed package   : python3-apt_1.1.0~beta1ubuntu0.16.04.8
```

133205 - Ubuntu 16.04 LTS / 18.04 LTS : python-apt vulnerabilities (USN-4247-1)**Synopsis**

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4247-1 advisory.

It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a machine-in-the-middle attack, this flaw could potentially be used to install altered packages. (CVE-2019-15795)

It was discovered that python-apt could install packages from untrusted repositories, contrary to expectations. (CVE-2019-15796)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4247-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.1 (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-2019-15795
CVE	CVE-2019-15796
XREF	USN:4247-1

Plugin Information

Published: 2020/01/23, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : python-apt-common_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python-apt-common_1.1.0~beta1ubuntu0.16.04.7

- Installed package : python3-apt_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python3-apt_1.1.0~beta1ubuntu0.16.04.7
```

129050 - Ubuntu 16.04 LTS / 18.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4136-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4136-1 advisory.

It was discovered that wpa_supplicant incorrectly handled certain management frames. 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-4136-1>

Solution

Update the affected packages.

Risk Factor

Low

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

3.3 (CVSS2#AV:A/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE-XREF [CVE-2019-16275](#)
USN:4136-1

Plugin Information

Published: 2019/09/19, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : wpasupplicant_2.4-0ubuntu6.3
- Fixed package : wpasupplicant_2.4-0ubuntu6.6
```

132931 - Ubuntu 16.04 LTS : Libgcrypt vulnerability (USN-4236-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4236-2 advisory.

USN-4236-1 fixed a vulnerability in Libgcrypt. This update provides the corresponding fix for Ubuntu 16.04 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-4236-2>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

6.3 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

5.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:L/AC:H/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE [CVE-2019-13627](#)
XREF USN:4236-2

Plugin Information

Published: 2020/01/15, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : libgcrypt20_1.6.5-2ubuntu0.5
- Fixed package : libgcrypt20_1.6.5-2ubuntu0.6

125725 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-4007-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4007-2 advisory.

USN-4007-1 fixed vulnerabilities in the Linux kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 18.04 LTS for Ubuntu 16.04 LTS.

Federico Manuel Bento discovered that the Linux kernel did not properly apply Address Space Layout Randomization (ASLR) in some situations for setuid a.out binaries. A local attacker could use this to improve the chances of exploiting an existing vulnerability in a setuid a.out binary.

As a hardening measure, this update disables a.out support.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4007-2>

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

2.5 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

1.9 (CVSS2#AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-11191
XREF	USN:4007-2

Plugin Information

Published: 2019/06/05, Modified: 2025/03/03

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-51-generic for this advisory.

140651 - Ubuntu 16.04 LTS : PulseAudio vulnerability (USN-4519-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4519-1 advisory.

Ratchanan Sirattanamet discovered that an Ubuntu-specific patch caused PulseAudio to incorrectly handle memory under certain error conditions in the Bluez 5 module. An attacker could use this issue to cause PulseAudio to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2020-15710)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-4519-1>

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H)

CVSS v3.0 Temporal Score

5.3 (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-2020-15710
XREF USN:4519-1

Plugin Information

Published: 2020/09/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.10
- Fixed package : libpulse-mainloop-glib0_1:8.0-0ubuntu3.14

- Installed package : libpulse0_1:8.0-0ubuntu3.10
- Fixed package : libpulse0_1:8.0-0ubuntu3.14

- Installed package : libpulsedsp_1:8.0-0ubuntu3.10
- Fixed package : libpulsedsp_1:8.0-0ubuntu3.14

- Installed package : pulseaudio_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio_1:8.0-0ubuntu3.14

- Installed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-bluetooth_1:8.0-0ubuntu3.14

- Installed package : pulseaudio-module-x11_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-module-x11_1:8.0-0ubuntu3.14

- Installed package : pulseaudio-utils_1:8.0-0ubuntu3.10
- Fixed package : pulseaudio-utils_1:8.0-0ubuntu3.14
```

18261 - Apache Banner Linux Distribution Disclosure**Synopsis**

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

Plugin Output

tcp/0

```
The Linux distribution detected was :
- Ubuntu 16.04 (xenial)
- Ubuntu 16.10 (yakkety)
```

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 : 2.4.18
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_authn_file
- mod_authn_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_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 - *:8000
```

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://10.84.42.93/  
Version : 2.4.99  
Source : Server: Apache/2.4.18 (Ubuntu)  
backported : 1  
os : ConvertedUbuntu
```

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/8000/www

```
URL : http://10.84.42.93:8000/  
Version : 2.4.99  
Source : Server: Apache/2.4.18 (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 : innoteck 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.

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/8000/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:16.04.6:~~lts~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.18 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:exiv2:libexiv2:0.25
cpe:/a:gnupg:libgcrypt:1.6.5 -> GnuPG Libgcrypt
cpe:/a:haxx:libcurl:7.47.0 -> Haxx libcurl
cpe:/a:jquery:jquery:1.11.3 -> jQuery
cpe:/a:jquery:jquery:1.12.4 -> jQuery
cpe:/a:mariadb:mariadb:10.0.38 -> MariaDB for Node.js
cpe:/a:openbsd:openssh:7.2 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:7.2p2 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssl:1.0.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.2g -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.1.1g -> OpenSSL Project OpenSSL
cpe:/a:php:php:7.2.32 -> PHP PHP
cpe:/a:samba:samba:4.3.11 -> Samba Samba
cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ
cpe:/a:vim:vim:7.4 -> Vim
x-cpe:/a:libbndp:libbndp:1.4

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 : photographer
photographer (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 :

- 127.0.0.1 (on interface lo)
- 10.84.42.93 (on interface enp0s3)

25202 - Enumerate IPv6 Interfaces via SSH**Synopsis**

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

The following IPv6 interfaces are set on the remote host :

```
- ::1 (on interface lo)
- 2409:40c0:1069:df43:2177:b4a9:6d53:2eb5 (on interface enp0s3)
- 2409:40c0:1069:df43:5a5a:11c0:4786:5a21 (on interface enp0s3)
- fe80::7a05:ae67:8ec7:fale (on interface enp0s3)
```

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 :

```
- 08:00:27:0a:3b:e9 (interface enp0s3)
```

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
enp0s3:
MAC : 08:00:27:0a:3b:e9
IPv4:
- Address : 10.84.42.93
Netmask : 255.255.255.0
Broadcast : 10.84.42.255
IPv6:
- Address : 2409:40c0:1069:df43:2177:b4a9:6d53:2eb5
Prefixlen : 64
Scope : global
- Address : fe80::7a05:ae67:8ec7:fa1e
Prefixlen : 64
Scope : link

```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information from the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```

Gateway Routes:
enp0s3:
ipv4_gateways:
10.84.42.175:
subnets:
- 0.0.0.0/0
ipv6_gateways:
fe80::4a2:97ff:fec8:6a88:
subnets:
- ::/0
Interface Routes:
enp0s3:
ipv4_subnets:
- 10.84.42.0/24
- 169.254.0.0/16
ipv6_subnets:
- 2409:40c0:1069:df43::/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.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

The following card manufacturers were identified :

08:00:27:0A:3B:E9 : 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:
- 08:00:27:0A:3B:E9

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/2.4.18 (Ubuntu)

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/8000/www

The remote web server type is :

Apache/2.4.18 (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: Sat, 01 Nov 2025 19:25:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Tue, 21 Jul 2020 09:32:32 GMT
ETag: "164f-5aaf04d7cd1a0"
Accept-Ranges: bytes
Content-Length: 5711
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

```
<!DOCTYPE HTML>
<!--
Photographer by v1n1v131r4
-->
<html>
<head>
<title>Photographer by v1n1v131r4</title>
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<link rel="stylesheet" href="assets/css/main.css" />
</head>
<body>

<!-- Header -->
<header id="header" class="alt">
<div class="logo"><a href="index.html">Photographer <span>by v1n1v131r4</span></a></div>
<a href="#menu">Menu</a>
</header>

<!-- Nav -->
<nav id="menu">
<ul class="links">
<li><a href="index.html">Home</a></li>
<li><a href="generic.html">Generic</a></li>
<li><a href="elements.html">Elements</a></li>
</ul>
</nav>

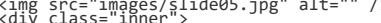
<!-- Banner -->
<section class="banner full">
<article>

<div class="inner">
<header>
<p>A prep OSCP machine by <a href="https://templated.co">v1n1v131r4</a></p>
<h2>Photographer</h2>
</header>
</div>
</article>
<article>

<div class="inner">
<header>
<p>Lorem ipsum dolor sit amet nullam feugiat</p>
<h2>Magna etiam</h2>
</header>
</div>
</article>
<article>

<div class="inner">
<header>
<p>Sed cursus aliquam veroeros lorem ipsum nullam</p>
<h2>Tempus dolor</h2>
</header>
</div>
</article>
<article>

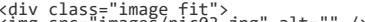
<div class="inner">
<header>
<p>Adipiscing lorem ipsum feugiat sed phasellus consequat</p>
```

```
<h2>Etiam feugiat</h2>
</header>
</div>
</article>
<article>

<div class="inner">
<header>
<p>Ipsum dolor sed magna veroeros lorem ipsum</p>
<h2>Lorem adipiscing</h2>
</header>
</div>
</article>
</section>

<!-- One -->
<section id="one" class="wrapper style2">
<div class="inner">
<div class="grid-style">

<div>
<div class="box">
<div class="image fit">

</div>
<div class="content">
<header class="align-center">
<p>maecenas sapien feugiat ex purus</p>
<h2>Lorem ipsum dolor</h2>
</header>
<p>Cras aliquet urna ut sapien tincidunt, quis malesuada elit facilisis. Vestibulum sit amet tortor velit. Nam elementum nibh a libero pharetra elementum. Maecenas feugiat ex purus, quis volutpat lacus placerat malesuada.</p>
<footer class="align-center">
<a href="#" class="button alt">Learn More</a>
</footer>
</div>
</div>
</div>

<div>
<div class="box">
<div class="image fit">

</div>
<div class="content">
<header class="align-center">
<p>mattis elementum sapien pretium tellus</p>
<h2>Vestibulum sit amet</h2>
</header>
<p>Cras aliquet urna ut sapien tincidunt, quis malesuada elit facilisis. Vestibulum sit amet tortor velit. Nam elementum nibh a libero pharetra elementum. Maecenas feugiat ex purus, quis volutpat lacus placerat malesuada.</p>
<footer class="align-center">
<a href="#" class="button alt">Learn More</a>
</footer>
</div>
</div>
</div>
</div>
</section>

<!-- Two -->
<section id="two" class="wrapper style3">
<div class="inner">
<header class="align-center">
<p>Nam vel ante sit amet libero scelerisque facilisis eleifend vitae urna</p>
<h2>Morbi maximus justo</h2>
</header>
</div>
</section>

<!-- Three -->
<section id="three" class="wrapper style2">
<div class="inner">
<header class="align-center">
<p>Nam vel ante sit amet libero scelerisque facilisis eleifend vitae urna</p>
<h2>Morbi maximus justo</h2>
</header>
<div class="gallery">
<div>
<div class="image fit">
!\[\]\(b5e678606b7e7d6985c138774510462b\_img.jpg\)
</div>
</div>
<div>
<div class="image fit">
!\[\]\(ff143afa08064eccb7b974fc848ad5e5\_img.jpg\)
</div>
</div>
<div>
<div class="image fit">
!\[\]\(3ebb39f62b405af0e16cf2981e1e5467\_img.jpg\)
</div>
</div>
<div>
<div class="image fit">
!\[\]\(22e8626fc54d24493707baf126afc88b\_img.jpg\)
</div>
</div>
</div>
</div>
</div>
```

```

</div>
</div>
</div>
</section>

<!-- Footer -->
<footer id="footer">
<div class="container">
<ul class="icons">
<li><a href="#" class="icon fa-twitter"><span class="label">Twitter</span></a></li>
<li><a href="#" class="icon fa-facebook"><span class="label">Facebook</span></a></li>
<li><a href="#" class="icon fa-instagram"><span class="label">Instagram</span></a></li>
<li><a href="#" class="icon fa-envelope-o"><span class="label">Email</span></a></li>
</ul>
</div>
<div class="copyright">
&copy; Untitled. All rights reserved.
</div>
</footer>

<!-- Scripts -->
<script src="assets/js/jquery.min.js"></script>
<script src="assets/js/jquery.scrollTo_min.js"></script>
<script src="assets/js/skel.min.js"></script>
<script src="assets/js/util.js"></script>
<script src="assets/js/main.js"></script>

</body>
</html>

```

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/8000/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Sat, 01 Nov 2025 19:25:38 GMT

Server: Apache/2.4.18 (Ubuntu)

Last-Modified: Sat, 01 Nov 2025 19:15:55 GMT

ETag: "1264-6428d4fbe524e"

Accept-Ranges: bytes

Content-Length: 4708

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=utf-8

Response Body :

<!DOCTYPE html>

<html class="k-source-index k-lens-index">

<head>

<meta charset="utf-8">

<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">

<meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1">

```

<meta name="description" content="" />
<meta name="author" content="daisa ahomi" />
<meta name="keywords" content="photography, daisa ahomi" />
<title>daisa ahomi</title>

<link rel="stylesheet" type="text/css" href="/app/site/themes/common/css/reset.css?0.22.24"/>
<link rel="stylesheet" type="text/css" href="/app/site/themes/common/css/kicons.css?0.22.24"/>
<link rel="stylesheet" type="text/css" href="/storage/themes/elementary/css/kshare.css"/>
<link id="koken_settings_css_link" rel="stylesheet" type="text/css" href="/settings.css.lens" />

<!--[if IE]>
<script src="/app/site/themes/common/js/html5shiv.js"></script>
<![endif]-->
<meta name="generator" content="Koken 0.22.24" />
<meta name="theme" content="Elementary 1.7.2" />
<link href="/app/site/themes/common/css/mediaelement/mediaelementplayer.css?0.22.24" rel="stylesheet">

<script src="//ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/app/site/themes/common/js/jquery.min.js"></script>')</script>
<script src="/koken.js?0.22.24"></script>
<script>$K.location = $.extend($K.location, {"here": "\/", "parameters": {"page": 1, "url": "\/"}, "page_class": "k-source-index k-lens-index"});</script>
<link rel="alternate" type="application/atom+xml" title="daisa ahomi: All uploads" href="/feed/content/recent.rss" />
<link rel="alternate" type="application/atom+xml" title="daisa ahomi: Essays" href="/feed/essays/recent.rss" />
<link rel="alternate" type="application/atom+xml" title="daisa ahomi: Timeline" href="/feed/timeline/recent.rss" />

</head>
<body class="k-source-index k-lens-index">
<div id="container" class="nav-header">
<header class="top clearfix">
<span class="tagline">Your site tagline</span>
<h1><a href="/" class="k-nav-current" title="Home" data-koken-internal>daisa ahomi</a></h1>
</header>
<nav id="main">
<ul class="k-nav-list k-nav-root "><li><a class="k-nav-current" data-kOKEN-internal title="Home" href="/>Home</a></li><li><a data-kOKEN-internal title="Timeline" href="/timeline/">Timeline</a></li><li><a data-kOKEN-internal title="Albums" href="/albums/">Albums</a></li><li><a data-kOKEN-internal title="Content" href="/content/">Content</a></li><li><a data-kOKEN-internal title="Essays" href="/essays/">Essays</a></li></ul></nav>
<main>

<section>
<div id="home-slideshow">
<div id="pulse_77b5f99903c6a6b600408f41efa7ce47" class="k-pulse" style="clear:left;" data-pulse-group="default"></div>
<script>
var pulse = $K.pulse.register({id: 'pulse_77b5f99903c6a6b600408f41efa7ce47', options:
{"relative": 1, "jsvar": "pulse", "link_to": "advance", "fallbacktext": "No featured content found. Assign some in the Library.", "albumUrl": "\/albums\/:slug\/", "dataUrl": "\/api.php?\&features\>content\>draft:1"} })
</script>
<div id="ss_spinner"></div>
<div id="home-slideshow-text" style="display:none;">
<a id="home-slideshow-title-link" href="#"><h4 id="home-slideshow-title">&ampnbsp</h4></a>&ampnbsp&ampnbsp&ampnbsp<span id="home-slideshow-caption">&ampnbsp</span></div>
<script>
pulse.on('start', function() {
$('#ss_spinner').addClass('loading');
});
pulse.on('waiting', function(e) {
if(e) {
$('#ss_spinner').addClass('loading');
} else {
$('#ss_spinner').removeClass('loading');
}
});
pulse.on('dataloaded', function() {
$('#ss_spinner').removeClass('loading');
});
pulse.on('transitionstart', function(e) {
$('#home-slideshow-text').show();
$('#home-slideshow-title').html(e.data.title || e.data.filename);
$('#home-slideshow-caption').html(e.data.caption);
$('#home-slideshow-title-link').attr("href", e.data.url).attr("title", e.data.title || e.data.filename);
});
</script>
</section>

<section>
</section>

<section>
</section>

</main>
<footer class="bot">

<nav>
<ul class="k-nav-list k-nav-root "><li><a class="k-nav-current" data-kOKEN-internal title="Home" href="/>Home</a></li><li><a data-kOKEN-internal title="Albums" href="/albums/">Albums</a></li><li><a data-kOKEN-internal title="Content" href="/content/">Content</a></li><li><a data-kOKEN-internal title="Essays" href="/essays/">Essays</a></li></ul></nav>
@ daisa ahomi | <a href="http://koken.me" target="_blank" title="Koken - a free website publishing system developed for photographers">Built with Koken</a>
</footer>
</div><!-- close container -->
<script src="/app/site/themes/common/js/share.js?0.22.24"></script>
</body>
</html>

```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ enp0s3
+ IPv4
- Address : 10.84.42.93
Assign Method : dynamic
+ IPv6
- Address : 2409:40c0:1069:df43:2177:b4a9:6d53:2eb5
Assign Method : dynamic
- Address : 2409:40c0:1069:df43:5a5a:11c0:4786:5a21
Assign Method : dynamic
- Address : fe80::7a05:ae67:8ec7:fa1e
Assign Method : static
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80/www

```
URL : http://10.84.42.93/assets/js/jquery.min.js
Version : 1.11.3
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/8000/www

URL : <http://10.84.42.93:8000/app/site/themes/common/js/jquery.min.js>
Version : 1.12.4

Error(s) occurred during detection. Please enable plugin debugging for more information.

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

<https://gnupg.org/download/index.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of Libgcrypt:

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.6.5

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20.0.5
Version : 1.6.5

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 1.4-2ubuntu0.16.04.1 (via package manager)
Version : 1.4
Managed by OS : True

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 464M 0 464M 0% /dev
tmpfs 99M 6.5M 93M 7% /run
/dev/sda1 218G 5.0G 202G 3% /
tmpfs 493M 244K 493M 1% /dev/shm
tmpfs 5.0M 4.0K 5.0M 1% /run/lock
tmpfs 493M 0 493M 0% /sys/fs/cgroup
/dev/sda2 923M 73M 787M 9% /boot
/dev/sda4 266G 179M 253G 1% /home
tmpfs 99M 52K 99M 1% /run/user/1001
```

```
tmpfs 99M 0 99M 0% /run/user/1000
```

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sr0 11:0 1 1024M 0 rom
sda 8:0 0 500G 0 disk
└─sda4 8:4 0 270.1G 0 part /home
  ├─sda2 8:2 0 954M 0 part /boot
  └─sda3 8:3 0 8.4G 0 part [SWAP]
  └─sda1 8:1 0 220.6G 0 part /
```



```
$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=474784k,nr_inodes=118696,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=100912k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
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)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd)
pstree on /sys/fs/pstree type pstree (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
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/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugepages type cgroup (rw,nosuid,nodev,noexec,relatime,hugepages)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=35,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12755)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugepages on /dev/hugepages type hugepages (rw,relatime,pagesize=2M)
configfs on /sys/kernel/config type configfs (rw,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/sda2 on /boot type ext4 (rw,relatime,data=ordered)
/dev/sda4 on /home type ext4 (rw,relatime,data=ordered)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
tmpfs on /run/user/1001 type tmpfs (rw,nosuid,nodev,relatime,size=100912k,mode=700,uid=1001,gid=1001)
gvfsd-fuse on /run/user/1001/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1001,group_id=1001)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=100912k,mode=700,uid=1000,gid=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: EDT -0400
Via timedatectl: time zone: America/New_York (EDT, -0400)
Via /etc/timezone: America/New_York
Via /etc/localtime: EST5EDT,M3-2.0,M11.1.0
```

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 : agi
Home folder : /home/agi
Start script : /bin/bash
Groups : agi

User : daisa
Home folder : /home/osboxes
Start script : /bin/bash
Groups : daisa
lpadmin
cdrom
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
Start script : /usr/sbin/nologin
Groups : lp

User : mail
Home folder : /var/mail
Start script : /usr/sbin/nologin
Groups : mail

User : news
Home folder : /var/spool/news
Start script : /usr/sbin/nologin
Groups : news

User : uucp

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-timesync
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-timesync

User : systemd-network
Home folder : /run/systemd/netif
Start script : /bin/false
Groups : systemd-network

User : systemd-resolve
Home folder : /run/systemd/resolve
Start script : /bin/false
Groups : systemd-resolve

User : systemd-bus-proxy
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-bus-proxy

User : syslog
Home folder : /home/syslog
Start script : /bin/false
Groups : syslog
adm

User : _apt
Home folder : /nonexistent
Start script : /bin/false
Groups : nogroup

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : uidd
Home folder : /run/uidd
Start script : /bin/false
Groups : uidd

User : lightdm
Home folder : /var/lib/lightdm
Start script : /bin/false
Groups : lightdm

User : whoopsie
Home folder : /nonexistent
Start script : /bin/false
Groups : whoopsie

User : avahi-autoipd
Home folder : /var/lib/avahi-autoipd
Start script : /bin/false
Groups : avahi-autoipd

User : avahi
Home folder : /var/run/avahi-daemon
Start script : /bin/false
Groups : avahi

```
User : dnsmasq
Home folder : /var/lib/misc
Start script : /bin/false
Groups : nogroup
```

```
User : colord
Home folder : /var/lib/colord
Start script : /bin/false
Groups : colord
```

```
User : speech-dispatcher
Home folder : /var/run/speech-dispatcher
Start script : /bin/false
Groups : audio
```

```
User : hplip
Home folder : /var/run/hplip
Start script : /bin/false
Groups : lp
```

```
User : kernoops
Home folder : /
Start script : /bin/false
Groups : nogroup
```

```
User : pulse
Home folder : /var/run/pulse
Start script : /bin/false
Groups : pulse
```

audio

```
User : rtkit
Home folder : /proc
Start script : /bin/false
Groups : rtkit
```

```
User : saned
Home folder : /var/lib/saned
Start script : /bin/false
Groups : saned
```

scanner

```
User : usbmux
Home folder : /var/lib/usbmux
Start script : /bin/false
Groups : plugdev
```

```
User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql
```

```
User : sshd
Home folder : /var/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-10.0 (via package manager)
Version : 10.0.38
```

Managed : 1
 Product : MariaDB Client

tcp/0

Path : mariadb-server-10.0 (via package manager)
 Version : 10.0.38
 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-1-5-21-3693138109-3993630114-3057792995

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

The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu

The remote SMB Domain Name is : PHOTOGRAPHER

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 : \\PHOTOGRAPHER\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 : \\PHOTOGRAPHER\sambashare  
Local path : C:\home\agi\share  
Comment : Samba on Ubuntu  
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff  
FILE_GENERIC_READ: YES  
FILE_GENERIC_WRITE: YES  
FILE_GENERIC_EXECUTE: YES  
  
Share path : \\PHOTOGRAPHER\IPC$  
Local path : C:\tmp  
Comment : IPC Service (photographer 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\$
- sambashare
- 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 :

- SMBV1
- 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 : Photographer
Scan policy used : Advanced Scan
Scanner IP : 10.84.42.33
Port scanner(s) : netstat
Port range : 65535

```

Ping RTT : 246.403 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'daisa' 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 : 2025/11/1 19:24 UTC
Scan duration : 966 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

udp/68

Port 68/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

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

tcp/8000/www

Port 8000/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/33597

Port 33597/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/33734

Port 33734/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/52951

Port 52951/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/59014

Port 59014/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 16.04 Linux Kernel 4.4

Confidence level : 56

Method : MLSinFP

Type : unknown

Fingerprint : unknown

Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Confidence level : 95

Method : SSH

Type : general-purpose

Fingerprint : SSH:SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10

Remote operating system : Linux Kernel 4.15.0-45-generic

Confidence level : 99

Method : uname

Type : general-purpose

Fingerprint : uname:Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64

GNU/Linux

Remote operating system : Ubuntu 16.x

Confidence level : 85

Method : HTTP

Type : general-purpose

Fingerprint : unknown

Remote operating system : Linux

Confidence level : 59

Method : SinFP

Type : general-purpose

Fingerprint : SinFP:

P1:B10113:F0x12:W29200:00204ffff:M1460:

P2:B10113:F0x12:W28960:00204fffff0402080afffffff4445414401030307:M1460:

P3:B00000:F0x00:W0:00:M0

P4:191303_7_p=8000

```
Remote operating system : Linux Kernel 4.15.0-45-generic on Ubuntu 16.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.15.0-45-generic on Ubuntu 16.04
Confidence level : 100
Method : LinuxDistribution
```

The remote host is running Linux Kernel 4.15.0-45-generic on Ubuntu 16.04

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 photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
```

Local checks have been enabled for this host.

```
The remote Debian system is :
stretch/sid
```

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 7.939121 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 : daisa
Protocol : SSH

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

Service : ssh
Version : 7.2p2
Banner : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 5 installs of OpenSSL:

Path : /usr/bin/openssl
Version : 1.0.2g
Associated Package : openssl 1.0.2g-1ubuntu4.14
Managed by OS : True

Path : /lib/x86_64-linux-gnu/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0

Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
Version : 1.1.1g
Associated Package : libssl1.1

Path : /usr/lib/x86_64-linux-gnu/libssl.so.1.1
Version : 1.1.1g
Associated Package : libssl1.1

Path : /lib/x86_64-linux-gnu/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libchill.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libtalla.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libhuron.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgmp.so

216936 - PHP Scripting Language Installed (Unix)

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.
Thorough test is required to get results on hosts running MacOS.

See Also

<https://www.php.net>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/php7.2
Version : 7.2.32
Associated Package : php7.2-cli: /usr/bin/php7.2
INI file : /etc/php/7.2/cli/php.ini
INI source : PHP binary grep
Managed by OS : True
```

179139 - Package Manager Packages Report (nix)**Synopsis**

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

Successfully retrieved and stored package data.

66334 - Patch Report**Synopsis**

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

. You need to take the following 573 actions :

[JQuery 1.2 < 3.5.0 Multiple XSS (136929)]

+ Action to take : Upgrade to JQuery version 3.5.0 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315)]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2 vulnerability (USN-6787-1) (198044)]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.

[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 : klirc vulnerabilities (USN-6736-1) (193362)]

+ Action to take : Update the affected klirc-utils, libklirc and / or libklirc-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 : Jinja2 vulnerabilities (USN-7343-1) (232645) }

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 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 / 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 / 24.10 : libxml2 vulnerabilities (USN-7302-1) (216780)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 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 / 24.10 : Python vulnerabilities (USN-7488-1) (235360)]

+ 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 : 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 / 18.04 LTS : Bind vulnerabilities (USN-6723-1) (193082)]

+ 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 : BusyBox vulnerabilities (USN-3935-1) (123751)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-3919-1) (183603)]

+ 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 : GD vulnerabilities (USN-3900-1) (122533)]

+ 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 : GNU C Library vulnerabilities (USN-6762-1) (194950)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6740-1) (193593)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7428-1) (234106)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7627-1) (241626)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2) (192577)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PolicyKit vulnerability (USN-3934-1) (123750)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Samba vulnerabilities (USN-7582-1) (240197)]

+ 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 : Wget vulnerabilities (USN-3943-1) (123973)]

+ Action to take : Update the affected wget and / or wget-udeb packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6944-2) (206015)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libvpx vulnerability (USN-7249-1) (214908)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libxml2 vulnerability (USN-6658-2) (191794)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ncurses vulnerability (USN-6684-1) (191736)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : poppler vulnerability (USN-3905-1) (183594)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : systemd vulnerability (USN-3938-1) (123930)]

+ Action to take : Update the affected packages.

[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 / 16.04 LTS : ImageMagick vulnerabilities (USN-7068-1) (209023)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 55 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3901-2) (122647)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3931-2) (123679)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 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 intel-microcode / or intel-microcode 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 : 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 : Jinja2 vulnerabilities (USN-6599-1) (189537)]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[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 : 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 : 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 ESM : AccountsService vulnerability (USN-6190-2) (181839)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : Apache HTTP Server vulnerability (USN-6510-1) (186221)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : Avahi vulnerability (USN-6129-2) (178778)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : Bind vulnerability (USN-6421-1) (182789)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : BusyBox vulnerabilities (USN-6335-1) (180472)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : CUPS vulnerability (USN-6361-2) (181883)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : FLAC vulnerability (USN-6360-2) (181769)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : GLib vulnerabilities (USN-6165-2) (183410)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : GNU binutils vulnerabilities (USN-6413-1) (182531)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Kerberos vulnerability (USN-6467-1) (184161)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : LibTIFF vulnerabilities (USN-6229-1) (178283)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6252-1) (178913)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6342-1) (180532)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6396-1) (181899)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6440-1) (183457)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6494-1) (186083)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6604-1) (189608)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerabilities (USN-6583-1) (188054)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : OpenLDAP vulnerability (USN-6197-1) (177901)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : OpenSSH vulnerabilities (USN-6560-2) (187955)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : OpenSSL vulnerabilities (USN-6435-1) (183384)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerabilities (USN-6513-1) (186226)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : Requests vulnerability (USN-6155-2) (177352)]

+ Action to take : Update the affected python-requests and / or python3-requests packages.

[Ubuntu 16.04 ESM / 18.04 ESM : X.Org X Server vulnerabilities (USN-6587-2) (189293)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : YAML vulnerabilities (USN-6233-1) (178443)]

+ 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 16.04 ESM / 18.04 ESM : curl vulnerability (USN-6429-2) (182932)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2) (183750)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : libcap2 vulnerability (USN-6166-2) (177431)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : libssh vulnerabilities (USN-6592-2) (189998)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : libx11 vulnerabilities (USN-6407-2) (182843)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : ncurses vulnerability (USN-6451-1) (183834)]

+ Action to take : Update the affected packages.

[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 : OpenSSL vulnerabilities (USN-6039-1) (174752)]

+ 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 / 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-5443-1) (161809)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 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).

11/25, 1:18 AM

Photographer

[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 python-mako and / or python3-mako packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PCRE vulnerabilities (USN-5425-1) (161249)]

+ 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 : 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 : libxml2 vulnerabilities (USN-6028-1) (174458)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[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 : 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 : GD library vulnerabilities (USN-5068-1) (153137)]

+ Action to take : Update the affected libgd-dev, libgd-tools and / or libgd3 packages.

+Impact : Taking this action will resolve 3 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 libsepol1, libsepol1-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 : libxml2 vulnerability (USN-5548-1) (163871)]
+ 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 : lxml vulnerability (USN-5225-1) (156650)]
+ Action to take : Update the affected python-lxml and / or python3-lxml packages.

[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 ESM / 18.04 LTS : Apache HTTP Server regression (USN-5487-3) (162515)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Cron regression (USN-5259-3) (160980)]
+ Action to take : Update the affected cron package.

[Ubuntu 16.04 ESM / 18.04 LTS : DjVuLibre vulnerability (USN-5005-1) (169510)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS : GLib vulnerability (USN-5189-1) (156040)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS : ICU vulnerability (USN-5133-1) (154903)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS : ImageMagick vulnerabilities (USN-5736-1) (168160)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4946-1) (149410)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4979-1) (150155)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5003-1) (150952)]

+ 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 : Linux kernel vulnerabilities (USN-5018-1) (151920)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5044-1) (152640)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5073-1) (153177)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5094-1) (153797)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5114-1) (154273)]

+ 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 : Linux kernel vulnerabilities (USN-5136-1) (154972)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5164-1) (155747)]

+ 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 : Linux kernel vulnerabilities (USN-5209-1) (156484)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5268-1) (157352)]
+ 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 : Linux kernel vulnerabilities (USN-5298-1) (158249)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5319-1) (158728)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5339-1) (159143)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5385-1) (160065)]
+ 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 : Linux kernel vulnerabilities (USN-5418-1) (161060)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5466-1) (161954)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5515-1) (163111)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5621-1) (165286)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5727-1) (167770)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5790-1) (169692)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

11/2/25, 1:18 AM

Photographer

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6095-1) (176227)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6130-1) (176565)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerability (USN-5357-1) (159372)]
+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 ESM / 18.04 LTS : OpenEXR vulnerability (USN-5150-1) (155655)]
+ Action to take : Update the affected libopenexr-dev, libopenexr22 and / or openexr packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : Perl vulnerability (USN-6112-1) (176458)]
+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS : libICE vulnerability (USN-5744-1) (168208)]
+ Action to take : Update the affected libice-dev and / or libice6 packages.

[Ubuntu 16.04 ESM / 18.04 LTS : shadow vulnerabilities (USN-5254-1) (157160)]
+ Action to take : Update the affected login, passwd and / or uidmap packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1) (164275)]
+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : APR vulnerability (USN-5056-1) (152918)]
+ Action to take : Update the affected libapr1 and / or libapr1-dev packages.

[Ubuntu 16.04 ESM : APR-util vulnerability (USN-5737-1) (168150)]
+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Apache HTTP Server vulnerability (USN-5942-2) (173277)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Apport vulnerabilities (USN-5077-2) (153366)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Avahi vulnerability (USN-5008-2) (151451)]
+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Bind vulnerabilities (USN-5747-1) (168280)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : BlueZ vulnerabilities (USN-4989-2) (150846)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : BusyBox vulnerability (USN-5179-2) (160896)]
+ Action to take : Update the affected packages.
[Ubuntu 16.04 ESM : CUPS vulnerability (USN-6128-2) (176561)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Cairo vulnerabilities (USN-5407-1) (160959)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Cron vulnerabilities (USN-5259-1) (157299)]
+ Action to take : Update the affected cron package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Cyrus SASL vulnerability (USN-5301-2) (158271)]
+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : DBD::mysql vulnerabilities (USN-5344-1) (183695)]
+ Action to take : Update the affected libdbd-mysql-perl package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : DBus vulnerability (USN-6372-1) (181452)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : DHCP vulnerabilities (USN-5658-2) (167065)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : DjVuLibre vulnerabilities (USN-4957-2) (149651)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Dnsmasq vulnerability (USN-4976-2) (164828)]
+ Action to take : Update the affected packages.
[Ubuntu 16.04 ESM : Expat vulnerability (USN-5638-1) (165463)]
+ Action to take : Update the affected packages.
[Ubuntu 16.04 ESM : FUSE vulnerability (USN-5326-1) (158939)]
+ Action to take : Update the affected fuse, libfuse-dev and / or libfuse2 packages.
[Ubuntu 16.04 ESM : FreeType vulnerability (USN-5453-1) (161671)]
+ Action to take : Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.

[Ubuntu 16.04 ESM : FriBidi vulnerabilities (USN-5922-1) (172131)]
+ 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 16.04 ESM : GCC vulnerability (USN-5770-1) (168518) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5768-1) (168533) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : GNU binutils vulnerability (USN-5349-1) (159248) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 150 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : GNU cpio vulnerability (USN-5064-2) (157224) ]
+ Action to take : Update the affected cpio package.

[ Ubuntu 16.04 ESM : GPT fdisk vulnerabilities (USN-5262-1) (157349) ]
+ Action to take : Update the affected gdisk package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1) (179902) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 ESM : Ghostscript vulnerability (USN-5618-1) (165278) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : GnuPG vulnerability (USN-5503-2) (163026) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 ESM : GnuTLS vulnerability (USN-5750-1) (168312) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 ESM : Graphite2 vulnerability (USN-5657-1) (165716) ]
+ Action to take : Update the affected libgraphite2-3 and / or libgraphite2-dev packages.

[ Ubuntu 16.04 ESM : Gzip vulnerability (USN-5378-4) (159725) ]
+ Action to take : Update the affected gzip package.

[ Ubuntu 16.04 ESM : HTTP-Daemon vulnerability (USN-5520-2) (163267) ]
+ Action to take : Update the affected libhttp-daemon-perl package.

[ Ubuntu 16.04 ESM : HarfBuzz vulnerability (USN-5746-1) (168234) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 ESM : ImageMagick vulnerabilities (USN-5855-4) (174409) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : Intel Microcode vulnerabilities (USN-5535-1) (163520) ]
+ Action to take : Update the affected intel-microcode package.
+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[ Ubuntu 16.04 ESM : JACK vulnerability (USN-5656-1) (165690) ]
+ Action to take : Update the affected packages.
```

[Ubuntu 16.04 ESM : Jinja2 vulnerability (USN-5701-1) (166558)]
+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.

[Ubuntu 16.04 ESM : LZ4 vulnerability (USN-4968-2) (150712)]
+ Action to take : Update the affected liblzf4-1, liblzf4-dev and / or liblzf4-tool packages.

[Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5841-1) (170966)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Libcroco vulnerabilities (USN-5389-1) (160213)]
+ 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 : Libgcrypt vulnerabilities (USN-5080-2) (153514)]
+ Action to take : Update the affected libgcrypt11-dev, libgcrypt20 and / or libgcrypt20-dev packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Libksba vulnerability (USN-5787-2) (169707)]
+ Action to take : Update the affected libksba-dev and / or libksba8 packages.
[Ubuntu 16.04 ESM : Libtasn1 vulnerability (USN-5707-1) (166748)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Libxslt vulnerabilities (USN-5575-2) (164326)]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel (HWE) vulnerabilities (USN-5883-1) (171812)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5560-2) (164016)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5669-2) (166006)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5757-2) (168344)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5981-1) (173618)]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Linux kernel vulnerability (USN-5591-1) (164538)]

11/2/25, 1:18 AM

Photographer

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-6060-2) (175288)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 38 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : NSS vulnerability (USN-5892-2) (172223)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : NTFS-3G vulnerability (USN-5711-2) (166940)]

+ Action to take : Update the affected ntfs-3g and / or ntfs-3g-dev packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Net-SNMP vulnerabilities (USN-5795-2) (170082)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : OpenEXR vulnerabilities (USN-4996-2) (150948)]

+ Action to take : Update the affected libopenexr-dev, libopenexr22 and / or openexr packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : OpenLDAP vulnerability (USN-5424-2) (161386)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : OpenSSH vulnerability (USN-5666-1) (166010)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-6188-1) (177537)]

+ Action to take : Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : PCRE vulnerabilities (USN-5665-1) (166014)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Perl DBI module vulnerabilities (USN-5030-2) (157372)]

+ Action to take : Update the affected libdbi-perl package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Pillow vulnerabilities (USN-5227-2) (156772)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : PolicyKit vulnerability (USN-5252-2) (157085)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Python vulnerability (USN-6394-1) (181767)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : QPDF vulnerabilities (USN-5026-2) (152178)]

+ Action to take : Update the affected libqpdf-dev, libqpdf21 and / or qpdf packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Rsyslog vulnerability (USN-5404-2) (161480)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : SQLite vulnerability (USN-5712-1) (166939)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Samba vulnerability (USN-5260-3) (157357)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Squashfs-Tools vulnerabilities (USN-5078-2) (153408)]

+ Action to take : Update the affected squashfs-tools package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Sudo vulnerabilities (USN-6005-2) (176456)]

+ Action to take : Update the affected sudo and / or sudo-ldap packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5836-1) (170913)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 64 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Vorbis vulnerabilities (USN-5420-1) (161171)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : WavPack vulnerability (USN-5721-1) (167272)]

+ Action to take : Update the affected libwavpack-dev, libwavpack1 and / or wavpack packages.

[Ubuntu 16.04 ESM : Wayland vulnerability (USN-5614-2) (165662)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5193-3) (178945)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5778-2) (171576)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : XZ Utils vulnerability (USN-5378-3) (159719)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : cups-filters vulnerability (USN-6083-2) (177429)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : curl vulnerabilities (USN-5964-2) (173432)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2) (161690)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : jbig2dec vulnerabilities (USN-5405-1) (160724)]

+ Action to take : Update the affected jbig2dec, libjbig2dec0 and / or libjbig2dec0-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXdmcp vulnerability (USN-5690-1) (166261)]

+ Action to take : Update the affected libxdmcp-dev and / or libxdmcp6 packages.

[Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1) (161452)]

+ Action to take : Update the affected libxfixes-dev and / or libxfixes3 packages.

[Ubuntu 16.04 ESM : libXi vulnerabilities (USN-5646-1) (165525)]

+ Action to take : Update the affected libxi-dev and / or libxi6 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXpm vulnerabilities (USN-5807-2) (171734)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXrandr vulnerabilities (USN-5428-1) (161330)]

+ Action to take : Update the affected libxrandr-dev and / or libxrandr2 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1) (161450)]

+ Action to take : Update the affected libxrender-dev and / or libxrender1 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1) (161630)]

+ Action to take : Update the affected libxv-dev and / or libxv1 packages.

[Ubuntu 16.04 ESM : libcdio vulnerabilities (USN-5558-1) (164012)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libjpeg-turbo vulnerabilities (USN-5553-1) (163922)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libpng vulnerabilities (USN-5432-1) (161447)]

+ Action to take : Update the affected libpng12-0, libpng12-dev and / or libpng3 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libamplerate vulnerability (USN-5749-1) (168279)]

+ Action to take : Update the affected libamplerate0, libamplerate0-dev and / or samplerate-programs packages.

[Ubuntu 16.04 ESM : libsndfile vulnerability (USN-5409-1) (160977)]

+ 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 16.04 ESM : libvpx vulnerabilities (USN-6403-3) (184162) ]
+ Action to take : Update the affected libvpx-dev, libvpx3 and / or vpx-tools packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2) (178444) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : libx11 vulnerability (USN-4966-2) (149905) ]
+ Action to take : Update the affected packages.
```

```
[ Ubuntu 16.04 ESM : libxml2 vulnerabilities (USN-5760-2) (168464) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : man-db vulnerability (USN-5334-1) (159026) ]
+ Action to take : Update the affected man-db package.

[ Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5477-1) (162173) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : pixman vulnerability (USN-5718-2) (168311) ]
+ Action to take : Update the affected libpixman-1-0 and / or libpixman-1-dev packages.
```

```
[ Ubuntu 16.04 ESM : protobuf vulnerabilities (USN-5769-1) (168509) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : rsync vulnerability (USN-5359-2) (162171) ]
+ Action to take : Update the affected rsync package.

[ Ubuntu 16.04 ESM : snapd vulnerabilities (USN-5292-3) (158162) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : systemd vulnerabilities (USN-5013-2) (151835) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : tcpdump vulnerabilities (USN-5331-1) (158987) ]
+ Action to take : Update the affected tcpdump package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM : util-linux vulnerability (USN-5478-1) (162221) ]
+ Action to take : Update the affected packages.
```

```
[ Ubuntu 16.04 ESM : zlib vulnerability (USN-5355-2) (159361) ]
+ 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 : CUPS vulnerability (USN-6844-1) (200879) ]
```

11/2/25, 1:18 AM

Photographer

+ 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 : 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 / 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).

11/25, 1:18 AM

Photographer

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : poppler vulnerability (USN-213-1) (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 : 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 : GD Graphics Library vulnerability (USN-7112-1) (211385)]

+ Action to take : Update the affected libgd-dev, libgd-tools and / or libgd3 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerability (USN-7015-3) (207976)]

+ 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 / 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-4359-1) (136608)]

+ Action to take : Update the affected packages.

[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 10 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 8 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 : CUPS vulnerabilities (USN-4340-1) (136029)]

+ 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 : DBus vulnerability (USN-4398-1) (137556)]

+ 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 : 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 : Evolution Data Server vulnerability (USN-4429-1) (138873)]

+ 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 : 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 159 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 Networking vulnerability (USN-4405-1) (137872)]

+ 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 34 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : ImageMagick vulnerabilities (USN-4670-1) (144300)]

+ 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 : Intel Microcode vulnerabilities (USN-4385-1) (137295)]

+ 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 : 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 vulnerabilities (USN-4434-1) (138999)]

+ 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 : 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-4441-1) (139181)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 30 different vulnerabilities (CVEs).

[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 14 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 : OpenEXR vulnerabilities (USN-4418-1) (138168)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4900-1) (148295)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4352-1) (136401)]

+ 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 : 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 : OpenSSL vulnerabilities (USN-4738-1) (148011)]

+ 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 : 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-4355-1) (136546)]

+ Action to take : Update the affected packages.

[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 : Python vulnerabilities (USN-4428-1) (138872)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 16 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 : SQLite vulnerabilities (USN-4394-1) (137353)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 39 different vulnerabilities (CVEs).

[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 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-4421-1) (138326)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 93 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 5 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.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : fwupd vulnerability (USN-4395-1) (137553)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : json-c vulnerability (USN-4360-4) (136964)]

+ 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 vulnerabilities (USN-4396-1) (137554)]

+ Action to take : Update the affected libexif-dev and / or libexif12 packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[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 : libjpeg-turbo vulnerability (USN-4386-1) (137296)]

+ 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 : 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.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[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 : lxml vulnerability (USN-4896-1) (148244)]

+ Action to take : Update the affected python-lxml and / or python3-lxml 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.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[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 vulnerabilities (USN-4424-1) (138552)]

+ 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 : 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.

11/2/25, 1:18 AM

Photographer

[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 16.04 LTS / 18.04 LTS / 20.04 LTS : xterm vulnerability (USN-4746-1) (147990)]

+ Action to take : Update the affected xterm package.

[Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-3) (207382)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Apport vulnerability (USN-4051-1) (126567)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Aspell vulnerability (USN-4155-1) (129967)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Berkeley DB vulnerability (USN-4004-1) (183607)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : BlueZ vulnerabilities (USN-4311-1) (135027)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Cyrus SASL vulnerability (USN-4256-1) (133352)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : DjVuLibre vulnerabilities (USN-4198-1) (131226)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Dnsmasq vulnerabilities (USN-6657-2) (193872)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Evince vulnerability (USN-3959-1) (183631)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Exiv2 vulnerability (USN-4270-1) (133524)]

+ Action to take : Update the affected exiv2, libexiv2-14 and / or libexiv2-dev packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Expat vulnerability (USN-4132-1) (128874)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : File Roller vulnerability (USN-4332-1) (135847)]

+ Action to take : Update the affected file-roller package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4032-1) (183605)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : GD Graphics Library vulnerabilities (USN-4316-1) (183650)]

+ Action to take : Update the affected libgd-dev, libgd-tools and / or libgd3 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : GLib vulnerability (USN-4049-1) (126565)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-4416-1) (138166)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : GNU cpio vulnerability (USN-4176-1) (130622)]

+ Action to take : Update the affected cpio and / or cpio-win32 packages.

[Ubuntu 16.04 LTS / 18.04 LTS : GStreamer Base Plugins vulnerability (USN-3958-1) (124408)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : GVfs vulnerabilities (USN-4053-1) (126598)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-7138-1) (212086)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : GnuTLS vulnerabilities (USN-3999-1) (125622)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : IBus vulnerability (USN-4134-3) (134888)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : ICU vulnerability (USN-4305-1) (134663)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : ImageMagick vulnerabilities (USN-4192-1) (131072)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 60 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Jinja2 vulnerabilities (USN-4011-1) (125771)]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : LibRaw vulnerabilities (USN-3989-1) (125337)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : LibTIFF vulnerabilities (USN-4158-1) (130052)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : LibreOffice vulnerability (USN-4138-1) (129351)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Libxs1t vulnerabilities (USN-4164-1) (130167)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux firmware vulnerability (USN-4351-1) (136400)]

+ Action to take : Update the affected linux-firmware, nic-firmware and / or scsi-firmware packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel update (USN-4041-1) (126374)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4017-1) (125998)]

+ 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 : Linux kernel vulnerabilities (USN-4094-1) (127889)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 32 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4115-1) (128475)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 28 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4135-1) (129049)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4144-1) (129490)]

+ 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 : Linux kernel vulnerabilities (USN-4162-1) (130151)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4185-1) (130965)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4210-1) (131564)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

11/25, 1:18 AM

Photographer

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4227-1) (132691)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4287-1) (133800)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4302-1) (134660)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4318-1) (135269)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4345-1) (136088)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4363-1) (136710)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4390-1) (137300)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4414-1) (138139)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4426-1) (138835)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4526-1) (140722)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4578-1) (141448)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4660-1) (143445)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4680-1) (144749)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4749-1) (147983)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4877-1) (147992)]

+ 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 : Linux kernel vulnerabilities (USN-4883-1) (147972)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4890-1) (148108)]

+ 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 : Linux kernel vulnerabilities (USN-4916-1) (148691)]

+ 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 : Linux kernel vulnerabilities (USN-6647-1) (190855)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6701-1) (192222)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6777-1) (197215)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6866-1) (201860)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6926-1) (204834)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 30 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6972-1) (206075)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 18 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7028-1) (207588)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7069-1) (209060)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 35 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7121-1) (211624)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 45 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7185-1) (213508)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 38 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7233-1) (214739)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7342-1) (232628)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 38 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7496-1) (235462)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 33 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7553-1) (237867)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7685-1) (243968)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability (USN-4710-1) (145518)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability (USN-7296-1) (216769)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerability and regression (USN-4185-3) (131013)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS / 18.04 LTS : NTFS-3G vulnerability (USN-3914-1) (183630)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : ORC vulnerability (USN-6964-2) (207999)]

+ Action to take : Update the affected liborc-0.4-0, liborc-0.4-dev and / or liborc-0.4-dev-bin packages.

[Ubuntu 16.04 LTS / 18.04 LTS : OpenSSH vulnerability (USN-7270-2) (216430)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4376-1) (136967)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4504-1) (140645)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-6632-1) (190449)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Patch vulnerabilities (USN-4071-1) (127042)]

+ Action to take : Update the affected patch package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Perl DBI module vulnerability (USN-4534-1) (140752)]

+ Action to take : Update the affected libdbi-perl package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4272-1) (133550)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4430-1) (138874)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : PyXDG vulnerability (USN-4700-1) (145081)]

+ Action to take : Update the affected python-xdg and / or python3-xdg packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Python 2.7 vulnerability (USN-4754-4) (147995)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Qt vulnerabilities (USN-4275-1) (133647)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : ReportLab vulnerability (USN-4273-1) (133551)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Samba vulnerability (USN-4510-1) (140640)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4150-1) (183629)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : Vim vulnerabilities (USN-4582-1) (183639)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

```
[ Ubuntu 16.04 LTS / 18.04 LTS : Wget vulnerability (USN-6852-2) (201110) ]
+ Action to take : Update the affected wget package.

[ Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerabilities (USN-7299-2) (232549) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : bzip2 vulnerabilities (USN-4038-1) (126305) ]
+ Action to take : Update the affected bzip2, libbz2-1.0 and / or libbz2-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6718-2) (192630) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : e2fsprogs vulnerability (USN-4249-1) (133225) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : elfutils vulnerabilities (USN-4012-1) (125811) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : file vulnerability (USN-4172-1) (130428) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : libarchive vulnerabilities (USN-4293-1) (134298) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : libbsd vulnerabilities (USN-4243-1) (133144) ]
+ Action to take : Update the affected libbsd-dev, libbsd0 and / or libbsd0-udeb packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : libndp vulnerability (USN-7248-1) (214886) ]
+ Action to take : Update the affected libndp-dev, libndp-tools and / or libndp0 packages.

[ Ubuntu 16.04 LTS / 18.04 LTS : libpcap vulnerability (USN-4221-1) (132016) ]
+ Action to take : Update the affected libpcap-dev, libpcap0.8 and / or libpcap0.8-dev packages.

[ Ubuntu 16.04 LTS / 18.04 LTS : librsvg vulnerabilities (USN-4436-1) (139024) ]
+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS / 18.04 LTS : libseccomp vulnerability (USN-4001-1) (125624) ]
+ Action to take : Update the affected libseccomp-dev, libseccomp2 and / or seccomp packages.

[ Ubuntu 16.04 LTS / 18.04 LTS : libsndfile vulnerabilities (USN-4013-1) (125812) ]
+ Action to take : Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).
```

[Ubuntu 16.04 LTS / 18.04 LTS : libsoup vulnerabilities (USN-7565-1) (238438)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : libvpx vulnerabilities (USN-4199-1) (131314)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : libxml2 vulnerabilities (USN-4274-1) (133646)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4042-1) (126375)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4646-1) (143266)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : python-apt vulnerabilities (USN-4247-1) (133205)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : rsync vulnerabilities (USN-4292-1) (134039)]

+ Action to take : Update the affected rsync package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : snapd vulnerabilities (USN-6940-2) (213997)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : systemd vulnerabilities (USN-4269-1) (133523)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : tcpdump vulnerabilities (USN-4252-1) (133291)]

+ Action to take : Update the affected tcpdump package.

+Impact : Taking this action will resolve 28 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : unzip vulnerabilities (USN-4672-1) (144337)]

+ Action to take : Update the affected unzip package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS : urllib3 vulnerabilities (USN-3990-1) (125338)]

+ 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 LTS / 18.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4136-1) (129050)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : AppArmor update (USN-4008-2) (125767)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : Apport vulnerabilities (USN-6894-1) (202245)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Bash vulnerability (USN-4058-1) (126748)]

+ Action to take : Update the affected bash, bash-builtins and / or bash-static packages.

[Ubuntu 16.04 LTS : Bind vulnerabilities (USN-6909-3) (205642)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : BlueZ vulnerabilities (USN-7265-1) (216160)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : CUPS vulnerability (USN-7041-3) (208229)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : Dnsmasq vulnerabilities (USN-4924-1) (148938)]

+ Action to take : Update the affected dnsmasq, dnsmasq-base and / or dnsmasq-utils packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Evince vulnerability (USN-4067-1) (126947)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4637-2) (143127)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 35 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : FreeRDP vulnerabilities (USN-4382-1) (137178)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : FreeType vulnerability (USN-4126-1) (128630)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : GDK-PixBuf vulnerability (USN-3912-1) (123001)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : GNU C Library vulnerability (USN-7259-2) (215239)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : JasPer vulnerabilities (USN-4688-1) (144849)]

+ Action to take : Update the affected libjasper-dev, libjasper-runtime and / or libjasper1 packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

```
[ Ubuntu 16.04 LTS : Libgcrypt vulnerability (USN-4236-2) (132931) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3981-2) (125142) ]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4068-2) (126949) ]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4255-2) (133351) ]
+ Action to take : Update the affected kernel package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-4007-2) (125725) ]
+ Action to take : Update the affected kernel package.

[ Ubuntu 16.04 LTS : OpenSSH vulnerability (USN-6560-3) (207279) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 LTS : PulseAudio vulnerability (USN-4519-1) (140651) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 LTS : cups-filters vulnerability (USN-7043-3) (208231) ]
+ Action to take : Update the affected packages.

[ Ubuntu 16.04 LTS : libsndfile vulnerability (USN-7267-1) (216330) ]
+ Action to take : Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.
+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[ Ubuntu 16.04 LTS : python-cryptography vulnerability (USN-6673-2) (192115) ]
+ Action to take : Update the affected python-cryptography and / or python3-cryptography packages.

[ Ubuntu 16.04 LTS : zlib vulnerabilities (USN-4246-1) (133204) ]
+ Action to take : Update the affected packages.
+Impact : Taking this action will resolve 4 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 :

- 2409:40c0:1069:df43:2177:b4a9:6d53:2eb5
- 2409:40c0:1069:df43:5a5a:11c0:4786:5a21

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-ettm@openssh.com
hmac-sha2-256
hmac-sha2-256-ettm@openssh.com
hmac-sha2-512
hmac-sha2-512-ettm@openssh.com
umac-128-ettm@openssh.com
umac-128@openssh.com
umac-64-ettm@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-ettm@openssh.com
hmac-sha2-256
hmac-sha2-256-ettm@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@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
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 : daisa
Commands failed due to lack of privilege escalation :

- Escalation account : (none)
Escalation method : (none)

Plugins :
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34998
Plugin Name : BIOS Info (SSH)

- Command : "LC_ALL=C dmidecode"
Response : "# dmidecode 3.0\nScanning /dev/mem for entry point."
Error : "\nCould not chdir to home directory /home/osboxes: No such file or
directory\n\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\ndevice/mem: Permission denied"

- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 3.0\nScanning /dev/mem for entry point."
Error : "\nCould not chdir to home directory /home/osboxes: No such file or
directory\n\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\ndevice/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\ndevice/mem: Permission denied"
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory"

- Plugin Filename : enumerate_occi_nix.nasl
Plugin ID : 154138
```

11/2/25, 1:18 AM

Photographer

```
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C dmidecode -s chassisasset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory"
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassisasset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory"
- Plugin Filename : linux_kernel_speculative_execution_detect.nbin
Plugin ID : 125216
Plugin Name : Processor Speculative Execution Vulnerabilities (Linux)
- Command : "head /sys/kernel/debug/x86/pti_enabled"
Response : null
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory\n\nhead: \ncannot open '/sys/kernel/debug/x86/pti_enabled' for reading: Permission denied"
- Command : "head /sys/kernel/debug/x86/retp_enabled"
Response : null
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory\n\nhead: \ncannot open '/sys/kernel/debug/x86/retp_enabled' for reading\n\n: Permission denied"
- Plugin Filename : localusers_pwexpiry.nasl
Plugin ID : 83303
Plugin Name : Unix / Linux - Local Users Information : Passwords Never Expire
- Command : "cat /etc/shadow"
Response : null
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory\n\nncat: /etc/shadow: Permission denied"
- Plugin Filename : ssh_get_info2.nasl
Plugin ID : 97993
Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
- Command : "lsmod | grep -q iptable_filter && iptables -L -n -v -t filter"
Response : null
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory\n\niptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)\n\nPerhaps iptables or your kernel needs to be upgraded."
- Command : "lsmod | grep -q _conntrack_ipv4 && iptables -L -n -v -t nat"
Response : null
Error : "\nCould not chdir to home directory /home/osboxes: No such file or directory\n\niptables v1.6.0: can't initialize iptables table `nat': Permission denied (you must be root)\n\nPerhaps iptables or your kernel needs to be upgraded."
```

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

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF

IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
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

104887 - Samba Version**Synopsis**

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

The remote Samba Version is : Samba 4.3.11-Ubuntu

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)**Synopsis**

The remote host supports the SMBv1 protocol.

Description

The remote host (Windows and/or Samba server) supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, most security and compliance agencies recommend that users disable SMBv1 per SMB best practices.

See Also

<http://www.nessus.org/u?59bfc3ef>
<http://www.nessus.org/u?b9d9ebf9>
<http://www.nessus.org/u?8dcab5e4>
<http://www.nessus.org/u?234f8ef8>
<http://www.nessus.org/u?4c7e0cf3>

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2025/08/13

Plugin Output

tcp/445/cifs

The remote host supports SMBv1.

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.

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/8000/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, 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 a11y-profile-manager-indicator 0.1.10-0ubuntu3 amd64 Accessibility Profile Manager - Unity desktop indicator
ii account-plugin-facebook 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon - facebook
ii account-plugin-flickr 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon - flickr
ii account-plugin-google 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon
ii accountsservice 0.6.40-2ubuntu11.3 amd64 query and manipulate user account information
ii acl 2.2.52-3 amd64 Access control list utilities
ii acpi-support 0.142 amd64 scripts for handling many ACPI events
ii acpid 1:2.0.26-1ubuntu2 amd64 Advanced Configuration and Power Interface event daemon
ii activity-log-manager 0.9.7-0ubuntu23.16.04.1 amd64 blacklist configuration user interface for Zeitgeist
ii adduser 3.113+nmu3ubuntu4 all add and remove users and groups
ii adium-theme-ubuntu 0.3.4-0ubuntu1.1 all Adium message style for Ubuntu
ii adwaita-icon-theme 3.18.0-2ubuntu3.1 all default icon theme of GNOME (small subset)
ii aisleriot 1:3.18.2-1ubuntu1 amd64 GNOME solitaire card game collection
ii alsa-base 1.0.25+dfsg-0ubuntu5 all ALSA driver configuration files
ii alsa-utils 1.1.0-0ubuntu5 amd64 Utilities for configuring and using ALSA
ii amd64-microcode 3.20180524.1-ubuntu0.16.04.2 amd64 Processor microcode firmware for AMD CPUs
ii anacron 2.3-23 amd64 cron-like program that doesn't go by time
ii apache2 2.4.18-2ubuntu3.15 amd64 Apache HTTP Server
ii apache2-bin 2.4.18-2ubuntu3.15 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.18-2ubuntu3.15 all Apache HTTP Server (common files)
ii apache2-utils 2.4.18-2ubuntu3.15 amd64 Apache HTTP Server (utility programs for web servers)
ii aptg 2.2.3.dfsg.1-2ubuntu1 amd64 Automated Password Generator - Standalone version
ii app-install-data 15.10 all Ubuntu applications (data files)
ii app-install-data-partner 16.04 all Application Installer (data files for partner applications/repositories)
ii apparmor 2.10.95-0ubuntu2.10 amd64 user-space parser utility for AppArmor
ii appmenu-qt 0.2.7+14.04.20140305-0ubuntu2 amd64 application menu for Qt
ii appmenu-qt5 0.3.0+16.04.20170216-0ubuntu1 amd64 application menu for Qt5
ii apport 2.20.1-0ubuntu2.18 all automatically generate crash reports for debugging
ii apport-gtk 2.20.1-0ubuntu2.18 all GTK+ frontend for the apport crash report system
ii apport-symptoms 0.20 all symptom scripts for apport
ii appstream 0.9.4-1ubuntu4 amd64 Software component index
ii apt 1.2.29ubuntu0.1 amd64 commandline package manager
ii apt-transport-https 1.2.29ubuntu0.1 amd64 https download transport for APT
ii apt-utils 1.2.29ubuntu0.1 amd64 package management related utility programs
ii aptdaemon 1.1.1+bzr982-0ubuntu14 all transaction based package management service
ii aptdaemon-data 1.1.1+bzr982-0ubuntu14 all data files for clients
ii apturl 0.5.2ubuntu11.2 amd64 install packages using the apt protocol - GTK+ frontend
ii apturl-common 0.5.2ubuntu11.2 amd64 install packages using the apt protocol - common data
ii aspell 0.60.7~20110707-3build1 amd64 GNU Aspell spell-checker
ii aspell-en 7.1-6.1.1 all English dictionary for GNU Aspell
ii at-sp2-core 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider Interface (dbus core)
ii attr 1:2.4.47-2 amd64 Utilities for manipulating filesystem extended attributes
ii avahi-autoipd 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi IPv4LL network address configuration daemon
ii avahi-daemon 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi mDNS/DNS-SD daemon
ii avahi-utils 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi browsing, publishing and discovery utilities
ii btrfs-dæmon 0.5.3~bzr0+16.04.20180209-0ubuntu1 amd64 Window matching library - dæmon
ii baobab 3.18.1-1ubuntu1 amd64 GNOME disk usage analyzer
ii base-files 9.4ubuntu4.8 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.39 amd64 Debian base system master password and group files
ii bash 4.3-14ubuntu1.2 amd64 GNU Bourne Again SHell
ii bash-completion 1:2.1.4-2ubuntu1.1 all programmable completion for the bash shell
ii bc 1.06.95-9build1 amd64 GNU bc arbitrary precision calculator language
ii bind9-host 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 Version of 'host' bundled with BIND 9.X
ii binutils 2.26.1-1ubuntu1.16.04.8 amd64 GNU assembler, linker and binary utilities
ii bluez 5.37-0ubuntu5.1 amd64 Bluetooth tools and daemons
ii bluez-cups 5.37-0ubuntu5.1 amd64 Bluetooth printer driver for CUPS
ii bluez-obexd 5.37-0ubuntu5.1 amd64 bluez obex daemon
ii branding-ubuntu 0.8 all Replacement artwork with Ubuntu branding
ii brltty 5.3.1-2ubuntu2.1 amd64 Access software for a blind person using a braille display
ii bsdmainutils 9.0.6ubuntu3 amd64 Collection of more utilities from FreeBSD
ii bsduutils 1:2.27.1-6ubuntu3.6 amd64 basic utilities from 4.4BSD-Lite
ii build-essential 12.1ubuntu2 amd64 Informational list of build-essential packages
ii busybox-initramfs 1:1.22.0-15ubuntu1 amd64 Standalone shell setup for initramfs
ii busybox-static 1:1.22.0-15ubuntu1 amd64 Standalone rescue shell with tons of builtin utilities
ii bzip2 1.0.6-8 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20170717-16.04.2 all Common CA certificates
ii checkbox-converged 1.2.4-0ubuntu1 all testing tool for all Ubuntu devices
ii checkbox-gui 1.2.4-0ubuntu1 all QML based interface for checkbox (transitional package)
ii cheese 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam
ii cheese-common 3.18.1-2ubuntu3 all Common files for the Cheese tool to take pictures and videos
ii colord 1.2.12-1ubuntu1 amd64 system service to manage device colour profiles -- system daemon
ii colord-data 1.2.12-1ubuntu1 all system service to manage device colour profiles -- data files
ii command-not-found 0.3ubuntu16.04.2 all Suggest installation of packages in interactive bash sessions
ii command-not-found-data 0.3ubuntu16.04.2 amd64 Set of data files for Command-not-found.
ii compiz 1:0.9.12.3+16.04.20180221-0ubuntu1 all OpenGL window and compositing manager
ii compiz-core 1:0.9.12.3+16.04.20180221-0ubuntu1 amd64 OpenGL window and compositing manager
ii compiz-gnome 1:0.9.12.3+16.04.20180221-0ubuntu1 amd64 OpenGL window and compositing manager - GNOME window decorator
ii compiz-plugins-default 1:0.9.12.3+16.04.20180221-0ubuntu1 amd64 OpenGL window and compositing manager - default plugins
ii console-setup 1.108ubuntu15.4 all console font and keymap setup program
ii console-setup-linux 1.108ubuntu15.4 all Linux specific part of console-setup
ii coreutils 8.25-2ubuntu3~16.04 amd64 GNU core utilities
ii cpio 2.11+dfsg-5ubuntu1 amd64 GNU cpio -- a program to manage archives of files
ii cpp 4.5.3.1-1ubuntu1 amd64 GNU C preprocessor (cpp)
ii cpp-5 5.4.0-6ubuntu1~16.04.11 amd64 GNU C preprocessor
ii cracklib-runtime 2.9.2-1ubuntu1 amd64 runtime support for password checker library cracklib2
ii crda 3.13-1 amd64 Wireless Central Regulatory Domain Agent
ii cron 3.0p11-12ubuntu2 amd64 process scheduling daemon
ii cups 2.1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - PPD/driver support, web interface
ii cups-browsed 1.8.3-2ubuntu3.4 amd64 OpenPrinting CUPS Filters - cups-browsed
ii cups-browsed 2.1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - BSD commands
ii cups-client 2.1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - client programs (SysV)
ii cups-common 2.1.3-4ubuntu0.7 all Common UNIX Printing System(tm) - common files
ii cups-core-drivers 2.1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - PPD-less printing
ii cups-daemon 2.1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - daemon
ii cups-filters 1.8.3-2ubuntu3.4 amd64 OpenPrinting CUPS Filters - Main Package
```

```

ii cups-filters-core-drivers 1.6.5-2ubuntu0.4 amd64 OpenPrinting CUPS filters - process printing
ii cups-pk-helper 0.2.5-2ubuntu2 amd64 PolicyKit helper to configure cups with fine-grained privileges
ii cups-ppdc 2:1.3-4ubuntu0.7 amd64 Common UNIX Printing System(tm) - PPD manipulation utilities
ii cups-server-common 2:1.3-4ubuntu0.7 all Common UNIX Printing System(tm) - server common files
ii dash 0.5.8-2.1ubuntu2 amd64 POSIX-compliant shell
ii dbus 1:10.6-1ubuntu3.3 amd64 simple interprocess messaging system (daemon and utilities)
ii dbus-x11 1:10.6-1ubuntu3.3 amd64 simple interprocess messaging system (X11 deps)
ii dc 1.06.95-9build1 amd64 GNU dc arbitrary precision reverse-polish calculator
ii dconf-cli 0.24.0-2 amd64 simple configuration storage system - utilities
ii dconf-gsettings-backend 0.24.0-2 amd64 simple configuration storage system - GSettings back-end
ii dconf-service 0.24.0-2 amd64 simple configuration storage system - D-Bus service
ii debconf 1.5.58ubuntu1 all Debian configuration management system
ii debconf-i18n 1.5.58ubuntu1 all full internationalization support for debconf
ii debianutils 4.7 amd64 Miscellaneous utilities specific to Debian
ii deja-dup 34.2-0ubuntu0.1 amd64 Back up your files
ii desktop-file-utils 0.22-1ubuntu5.2 amd64 Utilities for .desktop files
ii dh-python 2.2015103ubuntu1.1 all Debian helper tools for packaging Python libraries and applications
ii dictionaries-common 1.26.3 all spelling dictionaries - common utilities
ii diffstat 1.61-1 amd64 produces graph of changes introduced by a diff file
ii diffutils 1:3.3-3 amd64 File comparison utilities
ii dirmngr 2:1.11-6ubuntu2.1 amd64 server for managing certificate revocation lists
ii distro-info-data 0.28ubuntu0.9 all information about the distributions' releases (data files)
ii dmidecode 3.0-2ubuntu0.1 amd64 SMBIOS/DMI table decoder
ii dmz-cursor-theme 0.4.4ubuntu1 all Style neutral, scalable cursor theme
ii dns-root-data 2018013001~16.04.1 all DNS root data including root zone and DNSSEC key
ii dnsmasq-base 2.75-1ubuntu0.16.04.5 amd64 Small caching DNS proxy and DHCP/TFTP server
ii dnsutils 1:9.10.3-dfsg.P4-8ubuntu1.12 amd64 Clients provided with BIND
ii doc-base 0.10.7 all utilities to manage online documentation
ii dosfstools 3.0.28-2ubuntu0.1 amd64 utilities for making and checking MS-DOS FAT filesystems
ii dpkg 1.18.4ubuntu1.5 amd64 Debian package management system
ii dpkg-dev 1.18.4ubuntu1.5 all Debian package development tools
ii e2fslibs 1.42.13-1ubuntu1 amd64 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.42.13-1ubuntu1 amd64 ext2/ext3/ext4 file system utilities
ii ed 1.10-2 amd64 classic UNIX line editor
ii efibootmgr 0.12-4 amd64 Interact with the EFI Boot Manager
ii eject 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 amd64 ejects CDs and operates CD-Changers under Linux
ii emacs-common 2.0.8 all Common facilities for all Emacsen
ii enchant 1.6.0-10.1build2 amd64 Wrapper for various spell checker engines (binary programs)
ii eog 3.18.2-1ubuntu2.1 amd64 Eye of GNOME graphics viewer program
ii espeak-data 1.48.0+dfsg-2 amd64 Multi-lingual software speech synthesizer: speech data files
ii ethtool 1:4.5-1 amd64 display or change Ethernet device settings
ii evince 3.18.2-1ubuntu4.3 amd64 Document (PostScript, PDF) viewer
ii evince-common 3.18.2-1ubuntu4.3 all Document (PostScript, PDF) viewer - common files
ii evolution-data-server 3.18.5-1ubuntu1.1 amd64 evolution database backend server
ii evolution-data-server-common 3.18.5-1ubuntu1.1 all architecture independent files for Evolution Data Server
ii evolution-data-server-online-accounts 3.18.5-1ubuntu1.1 amd64 evolution data server integration with Ubuntu Online Accounts
ii example-content 49 all Ubuntu example content
ii fakeroot 1:20.2-1ubuntu1 amd64 tool for simulating superuser privileges
ii file 1:5.25-2ubuntu1.1 amd64 Determines file type using "magic" numbers
ii file-roller 3.16.5-0ubuntu1.2 amd64 archive manager for GNOME
ii findutils 4.6.0+git+20160126-2 amd64 utilities for finding files--find, xargs
ii firefox 65.0.1+build2-0ubuntu0.16.04.1 amd64 Safe and easy web browser from Mozilla
ii firefox-locale-en 65.0.1+build2-0ubuntu0.16.04.1 amd64 English language pack for Firefox
ii fontconfig 2.11.94-0ubuntu1.1 amd64 generic font configuration library - support binaries
ii fontconfig-config 2.11.94-0ubuntu1.1 all generic font configuration library - configuration
ii fonts-dejavu-core 2.35-1 all Vera font family derivative with additional characters
ii fonts-freefont-ttf 20120503-4 all Freefont Serif, Sans and Mono TrueType fonts
ii fonts-guru 2:1.2 all Meta package to install all Punjabi fonts
ii fonts-guru-extra 2.0-3 all Free fonts for Punjabi language
ii fonts-kacst 2.01+mry-12 all KACST free TrueType Arabic fonts
ii fonts-kacst-one 5.0+svn11846-7 all TrueType font designed for Arabic language
ii fonts-khmeros-core 5.0-7ubuntu1 all KhmerOS Unicode fonts for the Khmer language of Cambodia
ii fonts-lao 0.0.20060226-9 all TrueType font for Lao language
ii fonts-liberation 1.07.4-1 all Fonts with the same metrics as Times, Arial and Courier
ii fonts-iklуг-sinhala 0.6-3 all Unicode Sinhala font by Lanka Linux User Group
ii fonts-lohit-guru 2.5.3-2 all Lohit TrueType font for Punjabi Language
ii fonts-nanum 20140930-1 all Nanum Korean fonts
ii fonts-noto-cjk 1:1.1004+repack2-1~ubuntu1 all "No Tofu" font families with large Unicode coverage (CJK)
ii fonts-opensymbol 2:102.7+LibO5.1.6~rc2-0ubuntu1~xenial16 all OpenSymbol TrueType font
ii fonts-sil-abyssinica 1.500-1 all smart Unicode font for Ethiopian and Erythrean scripts (Amharic et al.)
ii fonts-sil-padauk 2.80-2 all smart Unicode font for languages in Myanmar
ii fonts-stix 1.1.1-4 all Scientific and Technical Information eXchange fonts
ii fonts-symbola 2.59-1 all symbolic font providing emoji characters from Unicode 7.0
ii fonts-takao-pgothic 003.02.01-9ubuntu3 all Japanese TrueType font set, Takao P Gothic Fonts
ii fonts-thai-tlwg 1:0.6.2-2.1 all Thai fonts maintained by TLWG (metapackage)
ii fonts-tibetan-machine 1.901b-5 all font for Tibetan, Dzongkha and Ladakhi (OpenType Unicode)
ii fonts-tlwg-garuda 1:0.6.2-2.1 all Thai Garuda font (dependency package)
ii fonts-tlwg-kinnari 1:0.6.2-2.1 all Thai Kinnari font (dependency package)
ii fonts-tlwg-kinnari-ttf 1:0.6.2-2.1 all Thai Kinnari TrueType font
ii fonts-tlwg-laksaman 1:0.6.2-2.1 all Thai Laksaman font (dependency package)
ii fonts-tlwg-laksaman-ttf 1:0.6.2-2.1 all Thai Laksaman TrueType font
ii fonts-tlwg-loma 1:0.6.2-2.1 all Thai Loma font (dependency package)
ii fonts-tlwg-loma-ttf 1:0.6.2-2.1 all Thai Loma TrueType font
ii fonts-tlwg-mono 1:0.6.2-2.1 all Thai TlwgMono font (dependency package)
ii fonts-tlwg-mono-ttf 1:0.6.2-2.1 all Thai TlwgMono TrueType font
ii fonts-tlwg-norasi 1:0.6.2-2.1 all Thai Norasi font (dependency package)
ii fonts-tlwg-norasi-ttf 1:0.6.2-2.1 all Thai Norasi TrueType font
ii fonts-tlwg-purisa 1:0.6.2-2.1 all Thai Purisa font (dependency package)
ii fonts-tlwg-purisa-ttf 1:0.6.2-2.1 all Thai Purisa TrueType font
ii fonts-tlwg-sawasdee 1:0.6.2-2.1 all Thai Sawasdee font (dependency package)
ii fonts-tlwg-sawasdee-ttf 1:0.6.2-2.1 all Thai Sawasdee TrueType font
ii fonts-tlwg-typewriter 1:0.6.2-2.1 all Thai TlwgTypewriter font (dependency package)
ii fonts-tlwg-typist 1:0.6.2-2.1 all Thai TlwgTypist font (dependency package)
ii fonts-tlwg-typist-ttf 1:0.6.2-2.1 all Thai TlwgTypist TrueType font
ii fonts-tlwg-typo 1:0.6.2-2.1 all Thai TlwgTypo font (dependency package)
ii fonts-tlwg-typo-ttf 1:0.6.2-2.1 all Thai TlwgTypo TrueType font
ii fonts-tlwg-umpush 1:0.6.2-2.1 all Thai Umpush font (dependency package)

```

```

ii fonts-tlwg-umpush-ttf 1:0.6.2-2.1 all Thai Umpush TrueType font
ii fonts-tlwg-waree 1:0.6.2-2.1 all Thai Waree font (dependency package)
ii fonts-tlwg-waree-ttf 1:0.6.2-2.1 all Thai Waree TrueType font
ii foomatic-db-compressed-ppds 20160212-0ubuntu1 all OpenPrinting printer support - Compressed PPDs derived from the database
ii friendly-recovery 0.2.31ubuntu2 all Make recovery more user-friendly
ii ftp 0.17-33 amd64 classical file transfer client
ii fuse 2.9.4-1ubuntu3.1 amd64 Filesystem_in_Userspace
ii fwupd 0.8.3-0ubuntu4 amd64 Firmware update daemon
ii fwupdate 0.5-2ubuntu7 amd64 Tools to manage UEFI firmware updates
ii fwupdate-signed 1.11.3+0.5-2ubuntu7 amd64 Linux Firmware Updater EFI signed binary
ii g++ 4:5.3.1-1ubuntu1 amd64 GNU C++ compiler
ii g++-5 5.4.0-6ubuntu1~16.04.11 amd64 GNU C++ compiler
ii gcc 4:5.3.1-1ubuntu1 amd64 GNU C compiler
ii gcc-5 5.4.0-6ubuntu1~16.04.11 amd64 GNU C compiler
ii gcc-5-base 5.4.0-6ubuntu1~16.04.11 amd64 GCC, the GNU Compiler Collection (base package)
ii gcc-6-base 6.0.1-0ubuntu1 amd64 GCC, the GNU Compiler Collection (base package)
ii gconf-service 3.2.6-3ubuntu6 amd64 GNOME configuration database system (D-Bus service)
ii gconf-service-backend 3.2.6-3ubuntu6 amd64 GNOME configuration database system (D-Bus service)
ii gconf2 3.2.6-3ubuntu6 amd64 GNOME configuration database system (support tools)
ii gconf2-common 3.2.6-3ubuntu6 all GNOME Configuration database system (common files)
ii gcr 3.18.0-1ubuntu1 amd64 GNOME crypto services (daemon and tools)
ii gdb 7.11.1-0ubuntu1~16.5 amd64 GNU Debugger
ii gdbserver 7.11.1-0ubuntu1~16.5 amd64 GNU Debugger (remote server)
ii gdisk 1.0.1-1build1 amd64 GPT fdisk text-mode partitioning tool
ii gedit 3.18.3-0ubuntu4 amd64 official text editor of the GNOME desktop environment
ii gedit-common 3.18.3-0ubuntu4 all official text editor of the GNOME desktop environment (support files)
ii genisoimage 9:1.1.11-3ubuntu1 amd64 Creates ISO-9660 CD-ROM filesystem images
ii geoclue 0.12.99-4ubuntu1 amd64 Geographic information framework
ii geooclue-ubuntu-geoip 1.0.2+14.04.20131125-0ubuntu2.16.04.1 amd64 Provide positioning for GeoClue via Ubuntu GeoIP services
ii geoip-database 20160408-1 all IP lookup command line tools that use the GeoIP library (country database)
ii gettext 0.19.7-2ubuntu3.1 amd64 GNU Internationalization utilities
ii gettext-base 0.19.7-2ubuntu3.1 amd64 GNU Internationalization utilities for the base system
ii ghostscript 9.26~dfsg+0~0ubuntu0.16.04.7 amd64 interpreter for the PostScript language and for PDF
ii ghostscript-x 9.26~dfsg+0~0ubuntu0.16.04.7 amd64 interpreter for the PostScript language and for PDF - X11 support
ii gir1.2-accounts-1.0 1.21+16.04.20160222-0ubuntu1 amd64 typelib file for libaccounts-glib0
ii gir1.2-appindicator3-0.1 12.10.1+16.04.20170215-0ubuntu1 amd64 Typelib files for libappindicator3-1.
ii gir1.2-atk-1.0 2.18.0-1 amd64 ATK accessibility toolkit (GObject_introspection)
ii gir1.2-atspi-2.0 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider (GObject_introspection)
ii gir1.2-dbusmenu-glib-0.4 16.04.1+16.04.20160927-0ubuntu1 amd64 typelib file for libdbusmenu-glib4
ii gir1.2-dee-1.0 1.2.7+15.04.20150304-0ubuntu2 amd64 GObject introspection data for the Dee library
ii gir1.2-freedesktop-1.46.0-3ubuntu1 amd64 Introspection data for some FreeDesktop components
ii gir1.2-gdata-0.0 0.17.4-1 amd64 GObject introspection data for the GData webservices library
ii gir1.2-gdkpixbuf-2.0 2.32.2-1ubuntu1.5 amd64 GDK_Pixbuf library - GObject-Introspection
ii gir1.2-glib-2.0 1.46.0-3ubuntu1 amd64 Introspection data for GLib, GObject, Gio and GModule
ii gir1.2-gnomekeyring-1.0 3.12.0-1build1 amd64 GNOME keyring services library - introspection data
ii gir1.2-goa-1.0 3.18.3-1ubuntu2 amd64 Introspection data for GNOME Online Accounts
ii gir1.2-gst-plugins-base-1.0 1.8.3-1ubuntu0.2 amd64 GObject introspection data for the GStreamer Plugins Base library
ii gir1.2-gstreamer-1.0 1.8.3-1~ubuntu0.1 amd64 GObject introspection data for the GStreamer library
ii gir1.2-gtk-3.0 3.18.9-1ubuntu3.3 amd64 GTK+ graphical user interface library -- gir bindings
ii gir1.2-gtksource-3.0 3.18.2-1 amd64 gir files for the GTK+ syntax highlighting widget
ii gir1.2-gudev-1.0 1:230-2 amd64 libgudev-1.0 introspection data
ii gir1.2ibus-1.0 1.5.11-1ubuntu2.1 amd64 Intelligent Input Bus - introspection data
ii gir1.2-javascriptcoregtk-4.0 2.20.5-0ubuntu0.16.04.1 amd64 JavaScript engine library from WebKitGTK+ - GObject introspection data
ii gir1.2-json-0.1 1.1.2~0ubuntu1 amd64 GLib JSON manipulation library (introspection data)
ii gir1.2-notify-0.7 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon (Introspection files)
ii gir1.2-packagekitglib-1.0 0.8.17-4ubuntu6~gcc5.4ubuntu1.4 amd64 GObject introspection data for the PackageKit GLib library
ii gir1.2-pango-1.0 1.38.1-1 amd64 Layout and rendering of internationalized text - gir bindings
ii gir1.2-peas-1.0 1.16.0-1ubuntu2 amd64 Application plugin library (introspection files)
ii gir1.2-rb-3.0 3.3-1ubuntu7 amd64 GObject introspection data for the rhythmbox music player
ii gir1.2-secret-1 0.18.4-1ubuntu2 amd64 Secret store (GObject-Introspection)
ii gir1.2-signon-1.0 1.13+16.04.20151209.1~0ubuntu1 amd64 GObject introspection data for the Signon library
ii gir1.2-soup-2.4 2.52.2-1ubuntu0.3 amd64 GObject introspection data for the libsoup HTTP library
ii gir1.2-totem-1.0 3.18.1-1ubuntu4 amd64 GObject introspection data for Totem media player
ii gir1.2-totem-piparser-1.0 3.18.6-1ubuntu1 amd64 GObject introspection data for the Totem Playlist Parser library
ii gir1.2-udisks-2.0 2.1.7-1ubuntu1 amd64 GObject based library to access udisks2 - introspection data
ii gir1.2-unity-5.0 7.1.4+16.04.20180209.1~0ubuntu1 amd64 GObject introspection data for the Unity library
ii gir1.2-vte-2.91 0.42.5-1ubuntu1 amd64 GObject introspection data for the VTE library
ii gir1.2-webkit2-4.0 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+ - GObject introspection data
ii gir1.2-wnck-3.0 3.14.1-2 amd64 GObject introspection data for the WNCK library
ii gkbd-capplet 3.6.0-1ubuntu2 amd64 GNOME control center tools for gkbofomekbd
ii glib-networking 2.48.2-1~ubuntu16.04.1 amd64 network-related giomodules for GLib
ii glib-networking-common 2.48.2-1~ubuntu16.04.1 all network-related giomodules for GLib - data files
ii glib-networking-services 2.48.2-1~ubuntu16.04.1 amd64 network-related giomodules for GLib - D-Bus services
ii gnome-accessibility-themes 3.18.0-2ubuntu2 all Accessibility themes for the GNOME desktop
ii gnome-bluetooth 3.18.2-1ubuntu2 amd64 GNOME Bluetooth tools
ii gnome-calculator 1:3.18.3-0ubuntu1.16.04.1 amd64 GNOME desktop calculator
ii gnome-calendar 3.20.4-0ubuntu0.1 amd64 Calendar application for GNOME
ii gnome-desktop3-data 3.18.2-1ubuntu1 all Common files for GNOME desktop apps
ii gnome-disk-utility 3.18.3.1-1ubuntu1.1 amd64 manage and configure disk drives and media
ii gnome-font-viewer 3.16.2-1ubuntu1 amd64 font viewer for GNOME
ii gnome-keyring 3.18.3-0ubuntu2.1 amd64 GNOME keyring services (daemon and tools)
ii gnome-mahjongg 1:3.18.0-1 amd64 classic Eastern tile game for GNOME
ii gnome-menus 3.13.3-6ubuntu3.1 amd64 GNOME implementation of the freedesktop menu specification
ii gnome-mines 1:3.18.2-2 amd64 popular minesweeper puzzle game for GNOME
ii gnome-orca 3.18.2-1ubuntu3 all Scriptable screen reader
ii gnome-power-manager 3.18.0-1ubuntu1 amd64 power management tool for the GNOME desktop
ii gnome-screensaver 3.6.1-7ubuntu4 amd64 GNOME screen saver and locker
ii gnome-screenshot 3.18.0-1ubuntu2 amd64 screenshot application for GNOME
ii gnome-session-bin 3.18.1.2-1ubuntu1.16.04.2 amd64 GNOME Session Manager - Minimal runtime
ii gnome-session-canberra 0.30.2-1ubuntu1 amd64 GNOME session log in and log out sound events
ii gnome-session-common 3.18.1.2-1ubuntu1.16.04.2 all GNOME Session Manager - common files
ii gnome-settings-daemon-schemas 3.18.2-0ubuntu3.1 all gnome-settings-daemon schemas
ii gnome-software 3.20.5-0ubuntu0.16.04.11 amd64 Software Center for GNOME
ii gnome-software-common 3.20.5-0ubuntu0.16.04.11 all Software Center for GNOME (common files)
ii gnome-sudoku 1:3.18.4-0ubuntu2 amd64 Sudoku puzzle game for GNOME
ii gnome-system-log 3.9.90-4 amd64 system log viewer for GNOME
ii gnome-system-monitor 3.18.2-1ubuntu1 amd64 Process viewer and system resource monitor for GNOME
ii gnome-terminal 3.18.3-1ubuntu1 amd64 GNOME terminal emulator application
ii gnome-terminal-data 3.18.3-1ubuntu1 all Data files for the GNOME terminal emulator

```

```

ii gnome-user-guide 3.18.1-1 all GNOME user's guide
ii gnome-user-share 3.14.2-2ubuntu4 amd64 User level public file sharing via WebDAV or ObexFTP
ii gnome-video-effects 0.4.1-3ubuntu1 all Collection of GStreamer effects
ii gnupg 1.4.20-1ubuntu3.3 amd64 GNU privacy guard - a free PGP replacement
ii gnupg-agent 2.1.11-6ubuntu1.1 amd64 GNU privacy guard - cryptographic agent
ii gnupg2 2.1.11-6ubuntu2.1 amd64 GNU privacy guard - a free PGP replacement (new v2.x)
ii gpgv 1.4.20-1ubuntu3.3 amd64 GNU privacy guard - signature verification tool
ii grep 2.25-1-16.04.1 amd64 GNU grep, egrep and fgrep
ii grilo-plugins-0.2-base 0.2.17-0ubuntu2 amd64 Framework for discovering and browsing media - Base Plugins
ii groff-base 1.22.3-7 amd64 GNU troff text-formatting system (base system components)
ii grub-common 2.02~beta2-36ubuntu3.20 amd64 GRand Unified Bootloader (common files)
ii grub-gfxpayload-lists 0.7 amd64 GRUB gfxpayload blacklist
ii grub-pc 2.02~beta2-36ubuntu3.20 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 2.02~beta2-36ubuntu3.20 amd64 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
ii grub2-common 2.02~beta2-36ubuntu3.20 amd64 GRand Unified Bootloader (common files for version 2)
ii gsettings-desktop-schemas 3.18.1-1ubuntu1 all GSettings desktop-wide schemas
ii gsettings-ubuntu-schemas 0.0.5+16.04.20160307-0ubuntu1 all GSettings desktop-wide schemas for Ubuntu
ii gsffonts 1:8.11+urwcyrl.0.7~pre44-4.2ubuntu1 all Fonts for the Ghostscript interpreter(s)
ii gstreamer1.0alsa 1.8.3-1ubuntu0.2 amd64 GStreamer plugin for ALSA
ii gstreamer1.0clutter-3.0 3.0.18-1 amd64 Clutter Plugin for GStreamer 1.0
ii gstreamer1.0-plugins-base 1.8.3-1ubuntu0.2 amd64 GStreamer plugins from the "base" set
ii gstreamer1.0-plugins-base-apps 1.8.3-1ubuntu0.2 amd64 GStreamer helper programs from the "base" set
ii gstreamer1.0-plugins-good 1.8.3-1ubuntu0.4 amd64 GStreamer plugins from the "good" set
ii gstreamer1.0-pulseaudio 1.8.3-1ubuntu0.4 amd64 GStreamer plugin for PulseAudio
ii gstreamer1.0-tools 1.8.3-1ubuntu0.1 amd64 Tools for use with GStreamer
ii gstreamer1.0-x 1.8.3-1ubuntu0.2 amd64 GStreamer plugins for X11 and Pango
ii gtk2-engines-murrine 0.98.2-0ubuntu2.2 amd64 cairo-based gtk+-2.0 theme engine
ii gucharmap 1:3.18.2-1ubuntu1 amd64 Unicode character picker and font browser
ii guile-2.0libs 2.0.11+1-10ubuntu0.1 amd64 Core Guile libraries
ii gvfs 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - GIO module
ii gvfs-backends 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - backends
ii gvfs-bin 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - binaries
ii gvfs-common 1.28.2-1ubuntu1~16.04.2 all userspace virtual filesystem - common data files
ii gvfs-daemons 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - servers
ii gvfs-fuse 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - fuse server
ii gvfs-libs 1.28.2-1ubuntu1~16.04.2 amd64 userspace virtual filesystem - private libraries
ii gzip 1.6-4ubuntu1 amd64 GNU compression utilities
ii hardening-includes 2.7ubuntu2 all Makefile for enabling compiler flags for security hardening
ii hdparm 9.48+ds-1ubuntu0.1 amd64 tune hard disk parameters for high performance
ii hicolor-icon-theme 0.15-0ubuntu1.1 all default fallback theme for FreeDesktop.org icon themes
ii hostname 3.16ubuntu2 amd64 utility to set/show the host name or domain name
ii hplip 3.16.3+repack0-1 amd64 HP Linux Printing and Imaging System (HPLIP)
ii hplip-data 3.16.3+repack0-1 all HP Linux Printing and Imaging - data files
ii hud 14.10+16.04.20160415-0ubuntu1 amd64 Backend for the Unity HUD
ii humanity-icon-theme 0.6.10.1 all Humanity Icon theme
ii hunspell-en-us 20070829-6ubuntu3 all English_american dictionary for hunspell
ii hwdata 0.267-1ubuntu2 all hardware identification / configuration data
ii hyphen-en-us 2.8.8-2ubuntu1 all US English hyphenation patterns for LibreOffice/OpenOffice.org
ii ibus 1.5.11-1ubuntu2.1 amd64 Intelligent Input Bus - core
ii ibus-gtk 1.5.11-1ubuntu2.1 amd64 Intelligent Input Bus - GTK+2 support
ii ibus-table 1.9.1-3ubuntu2 all table engine for IBus
ii ifupdown 0.8.10ubuntu1.4 amd64 high level tools to configure network interfaces
ii im-config 0.29-1ubuntu12.4 all Input method configuration framework
ii imagemagick 8:6.8.9.9-7ubuntu5.13 amd64 image manipulation programs -- binaries
ii imagemagick-6.q16 8:6.8.9.9-7ubuntu5.13 amd64 image manipulation programs -- quantum depth Q16
ii imagemagick-common 8:6.8.9.9-7ubuntu5.13 all image manipulation programs -- infrastructure
ii indicator-application 12.10.1+16.04.20170120-0ubuntu1 amd64 Application Indicators
ii indicator-appmenu 15.02.0+16.04.20151104-0ubuntu1 amd64 Indicator for application menus.
ii indicator-bluetooth 0.0.6+16.04.20160526-0ubuntu1 amd64 System bluetooth indicator.
ii indicator-datetime 15.10+16.04.20160406-0ubuntu1 amd64 Simple clock
ii indicator-keyboard 0.0.0+16.04.20151125-0ubuntu1 amd64 Keyboard indicator
ii indicator-messages 13.10.1+15.10.20150505-0ubuntu1 amd64 indicator that collects messages that need a response
ii indicator-power 12.10.6+16.04.20160105-0ubuntu1 amd64 Indicator showing power state.
ii indicator-printers 0.1.7+15.04.20150220-0ubuntu2 amd64 indicator showing active print jobs
ii indicator-session 12.10.5+16.04.20160412-0ubuntu1 amd64 indicator showing session management, status and user switching
ii indicator-sound 12.10.2+16.04.20160406-0ubuntu1 amd64 System sound indicator.
ii info 6.1.0.dfsg.1-5 amd64 Standalone GNU Info documentation browser
ii init 1.29ubuntu4 amd64 System-V-like init utilities - metapackage
ii init-system-helpers 1.29ubuntu4 all helper tools for all init systems
ii initramfs-tools 0.122ubuntu8.14 all generic modular initramfs generator (automation)
ii initramfs-tools-bin 0.122ubuntu8.14 amd64 binaries used by initramfs-tools
ii initramfs-tools-core 0.122ubuntu8.14 all generic modular initramfs generator (core tools)
ii initscripts 2.88dfsg-59.3ubuntu2 amd64 scripts for initializing and shutting down the system
ii inputattach 1:1.4.9-1 amd64 utility to connect serial-attached peripherals to the input subsystem
ii insserv 1.14.0-5ubuntu3 amd64 boot sequence organizer using LSB init.d script dependency information
ii install-info 6.1.0.dfsg.1-5 amd64 Manage installed documentation in info format
ii intel-gpu-tools 1.14-1 amd64 tools for debugging the Intel graphics driver
ii intel-microcode 3.20180807a.0ubuntu0.16.04.1 amd64 Processor microcode firmware for Intel CPUs
ii intltool-debian 0.35.0+20060710.4 all Help i18n of RFC822 compliant config files
ii ippusbxd 1.23-1 amd64 Daemon for IPP USB printer support
ii iproute2 4.3.0-1ubuntu3.16.04.4 amd64 networking and traffic control tools
ii iptables 1.6.0-2ubuntu3 amd64 administration tools for packet filtering and NAT
ii iputils-arping 3:20121221-5ubuntu2 amd64 Tool to send ICMP echo requests to an ARP address
ii iputils-ping 3:20121221-5ubuntu2 amd64 Tools to test the reachability of network hosts
ii iputils-tracepath 3:20121221-5ubuntu2 amd64 Tools to trace the network path to a remote host
ii irqbalance 1.1.0-2ubuntu1 amd64 Daemon to balance interrupts for SMP systems
ii isc-dhcp-client 4.3.3-5ubuntu12.10 amd64 DHCP client for automatically obtaining an IP address
ii isc-dhcp-common 4.3.3-5ubuntu12.10 amd64 common files used by all of the isc-dhcp packages
ii iso-codes 3.65-1 all ISO language, territory, currency, script codes and their translations
ii iucode-tool 1.5.1-1ubuntu0.1 amd64 Intel processor microcode tool
ii iw 3.17-1 amd64 tool for configuring Linux wireless devices
ii jayatana 2.7-0ubuntu5 amd64 Java Native Library for jayatana project
ii kbd 1.15.5-1ubuntu5 amd64 Linux console font and keytable utilities
ii kerneloops-daemon 0.12+git20140509-2ubuntu1 amd64 kernel oops tracker
ii keyboard-configuration 1.108ubuntu15.4 all system-wide keyboard preferences
ii klibc-utils 2.0.4-8ubuntu1.16.04.4 amd64 small utilities built with klibc for early boot
ii kmod 22-1ubuntu5.2 amd64 tools for managing Linux kernel modules
ii krb5-locales 1.13.2+dfsg-5ubuntu2.1 all Internationalization support for MIT Kerberos

```

```

ii language-pack-en 1:16.04+20161009 all translation updates for language English
ii language-pack-en-base 1:16.04+20160627 all translations for language English
ii language-pack-gnome-en 1:16.04+20161009 all GNOME translation updates for language English
ii language-pack-gnome-en-base 1:16.04+20160627 all GNOME translations for language English
ii language-selector-common 0.165.4 all Language selector for Ubuntu
ii language-selector-gnome 0.165.4 all Language selector for Ubuntu
ii laptop-detect 0.13.7ubuntu2 amd64 attempt to detect a laptop
ii less 481-2.1ubuntu0.2 amd64 pager program similar to more
ii liba11y-profile-manager-0.1-0 0.1.10-0ubuntu3 amd64 Accessibility profile manager - Shared library
ii liba11y-profile-manager-data 0.1.10-0ubuntu3 all Accessibility Profile Manager - GSettings data
ii libaa1 1.4p5-44build1 amd64 ASCII art library
ii libabw-0.1-1v5 0.1.1-2ubuntu2 amd64 library for reading and writing AbiWord(tm) documents
ii libaccount-plugin-1.0-0 0.1.8+16.04.20160201-0ubuntu1 amd64 libaccount-plugin for Unity Control Center
ii libaccount-plugin-generic-oauth 0.12+16.04.20160126-0ubuntu1 amd64 GNOME Control Center account plugin for single signon - generic OAuth
ii libaccount-plugin-google 0.12+16.04.20160126-0ubuntu1 amd64 GNOME Control Center account plugin for single signon - Google Auth
ii libaccounts-glib0 1.21+16.04.20160222-0ubuntu1 amd64 library for single signon
ii libaccounts-qt5-1 1.14+16.04.20151106.1-0ubuntu1 amd64 QT library for single sign on
ii libaccounts-service0 0.6.40-2ubuntu11.3 amd64 query and manipulate user account information - shared libraries
ii libacpi 2.2.52-3 amd64 Access control list shared library
ii libao1 0.3.110-2 amd64 Linux kernel AIO access library - shared library
ii libalgorithm-diff-perl 1.19.03-1 all module to find differences between files
ii libalgorithm-diff-xs-perl 0.04-4build1 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 libandroid-properties@ 0.1.0+git20150106+6d424c9-0ubuntu7 amd64 library to provide access to get, set and list Android properties
ii libao-common 1.1.0-3ubuntu1 all Cross Platform Audio Output Library (Common files)
ii libao4 1.1.0-3ubuntu1 amd64 Cross Platform Audio Output Library
ii libapache2-mod-php7.2 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapparmor-perl 2.10.95-0ubuntu2.10 amd64 AppArmor library Perl bindings
ii libapparmor1 2.10.95-0ubuntu2.10 amd64 changehat AppArmor library
ii libappindicator3-1 12.10.1+16.04.20170215-0ubuntu1 amd64 Application Indicators
ii libappstream-glib6 0.5.13-1ubuntu6 amd64 GNOME library to access AppStream services
ii libappstream3 0.9.4-1ubuntu4 amd64 Library to access AppStream services
ii libapr1 1.5.2-3 amd64 Apache Portable Runtime library
ii libaprutil1 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library
ii libaprutil1-db-sqlite3 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-inst2.0 1.2.29ubuntu0.1 amd64 deb package format runtime library
ii libapt-pkg-perl 0.1.29build7 amd64 Perl interface to libapt-pkg
ii libapt-pkg5.0 1.2.29ubuntu0.1 amd64 package management runtime library
ii libarchive-zip-perl 1.56-2ubuntu0.1 all Perl module for manipulation of ZIP archives
ii libarchive13 3.1.2-11ubuntu0.16.04.6 amd64 Multi-format archive and compression library (shared library)
ii libargon2-0 0-20161029-1+ubuntu16.04.1+deb.sury.org+1 amd64 memory-hard hashing function - runtime library
ii libert-2.0-2 2.3.21-2 amd64 Library of functions for 2D graphics - runtime files
ii libasan1 5.4.0-6ubuntu1-16.04.11 amd64 AddressSanitizer - a fast memory error detector
ii libasn1-8-heimdal 1.7-git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - ASN.1 library
ii libasound2 1.1.0-0ubuntu1 amd64 shared library for ALSA applications
ii libasound2-data 1.1.0-0ubuntu1 all Configuration files and profiles for ALSA drivers
ii libasound2-plugins 1.1.0-0ubuntu1 amd64 ALSA library additional plugins
ii libaspell15 0.60.7-20110707-3build1 amd64 GNU Aspell spell-checker runtime library
ii libasprintf-dev 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library development files
ii libasprintf0v5 0.19.7-2ubuntu3.1 amd64 GNU library to use fprintf and friends in C++
ii libassuan0 2.4.2-2 amd64 IPC library for the GnuPG components
ii libasyncns0 0.8-5build1 amd64 Asynchronous name service query library
ii libatasmart4 0.19-3 amd64 ATA S.M.A.R.T. reading and parsing library
ii libatk-adaptor 2.18.1-1ubuntu1 amd64 AT-SPI 2 toolkit bridge
ii libatk-bridge2.0-0 2.18.1-2ubuntu1 amd64 AT-SPI 2 toolkit bridge - shared library
ii libatk1.0-0 2.18.0-1 amd64 ATK accessibility toolkit
ii libatk1.0-data 2.18.0-1 all Common files for the ATK accessibility toolkit
ii libatkmm-1.6-1y5 2.24.2-1 amd64 C++ wrappers for ATK accessibility toolkit (shared libraries)
ii libatm1 1.2.5.1-1.5 amd64 shared library for ATM (Asynchronous Transfer Mode)
ii libatomic1 5.4.0-6ubuntu1-16.04.11 amd64 support library providing atomic built-in functions
ii libatspi2.0-0 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider Interface - shared library
ii libattr1 1:2.4.47-2 amd64 Extended attribute shared library
ii libaudio2 1.9.4-4 amd64 Network Audio System - shared libraries
ii libaudit-common 1:2.4.5-1ubuntu2.1 all Dynamic library for security auditing - common files
ii libaudit1 1:2.4.5-1ubuntu2.1 amd64 Dynamic library for security auditing
ii libauthen-sasl-perl 2.1600-1 all Authen::SASL X509 Authentication framework
ii libavahi-client3 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi client library
ii libavahi-common-data 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi common data files
ii libavahi-common3 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi common library
ii libavahi-core7 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi's embeddable mDNS/DNS-SD library
ii libavahi-glib1 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi GLib integration library
ii libavahi-ui-gtk3-0 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi GTK+ User interface library for GTK3
ii libavc1394-0 0.5.4-4 amd64 control IEEE 1394 audio/video devices
ii libbabeltrace-ctf1 1.3.2-1 amd64 Common Trace Format (CTF) library
ii libbabeltrace1 1.3.2-1 amd64 Babeltrace conversion libraries
ii libbamf3-2 0.5.3~bzr0+16.04.20180209-0ubuntu1 amd64 Window matching library - shared library
ii libbind9-140 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 BIND9 Shared Library used by BIND
ii libblkid1 2.27.1-6ubuntu3.6 amd64 block device ID library
ii libbluetooth3 5.37-0ubuntu5.1 amd64 Library to use the BlueZ Linux Bluetooth stack
ii libboost-date-time1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 set of date-time libraries based on generic programming concepts
ii libboost-filesystem1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 filesystem operations (portable paths, iteration over directories, etc) in C++
ii libboost-iostreams1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 Boost.Iostreams Library
ii libboost-system1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 Operating system (e.g. diagnostics support) library
ii libbrlapi0 0.6.5.1-2ubuntu2.1 amd64 braille display access via BRILTY - shared library
ii libbsds0 0.8.2-1 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-8 amd64 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.23-0ubuntu11 amd64 GNU C Library: Binaries
ii libc-dev-bin 2.23-0ubuntu11 amd64 GNU C Library: Development binaries
ii libc6 2.23-0ubuntu11 amd64 GNU C Library: Shared libraries
ii libc6-dbg 2.23-0ubuntu11 amd64 GNU C Library: detached debugging symbols
ii libc6-dev 2.23-0ubuntu11 amd64 GNU C Library: Development Libraries and Header Files
ii libcacad 0.99.beta19-2ubuntu0.16.04.1 amd64 colour ASCII art library
ii libcairo-gobject2 1.14.6-1 amd64 Cairo 2D vector graphics library (GObject library)
ii libcairo-perl 1.106-1build1 amd64 Perl interface to the Cairo graphics library
ii libcairo2 1.14.6-1 amd64 Cairo 2D vector graphics library
ii libcairoomm-1.0-1v5 1.12.0-1 amd64 C++ wrappers for Cairo (shared libraries)

```

```

ii libcamel-1.2-54 3.18.5-1ubuntu1.1 amd64 Evolution MIME message handling library
ii libcanberra-gtk-module 0.30-2.1ubuntu1 amd64 translates GTK+ widgets signals to event sounds
ii libcanberra-gtk0 0.30-2.1ubuntu1 amd64 GTK+ helper for playing widget event sounds with libcanberra
ii libcanberra-gtk3-module 0.30-2.1ubuntu1 amd64 translates GTK3 widgets signals to event sounds
ii libcanberra-pulse 0.30-2.1ubuntu1 amd64 PulseAudio backend for libcanberra
ii libcanberra0 0.30-2.1ubuntu1 amd64 simple abstract interface for playing event sounds
ii libcap-ng0 0.7.7-1 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.24-12 amd64 POSIX 1003.1e capabilities (library)
ii libcap2-bin 1:2.24-12 amd64 POSIX 1003.1e capabilities (utilities)
ii libcapnp-0.5.3~0.5.3-2ubuntu1.1 amd64 Cap'n Proto C++ library
ii libcc1-0 5.4.0~6ubuntu1~16.04.11 amd64 GCC cc1 plugin for GDB
ii libcdio-cdda1 0.83-4.2ubuntu1 amd64 Library to read and control digital audio CDs
ii libcdio-paranoia1 0.83-4.2ubuntu1 amd64 library to read digital audio CDs with error correction
ii libcdio13 0.83-4.2ubuntu1 amd64 library to read and control CD-ROM
ii libcdparanoia0 3.10.2+debian-11 amd64 audio extraction tool for sampling CDs (library)
ii libcdr-0.1-1 0.1.2-2ubuntu2 amd64 library for reading and converting Corel DRAW files
ii libcg-i-fast-perl 1:2.10-1 all CGI subclass for work with FCGI
ii libcg-i-pm-perl 4.26-1 all module for Common Gateway Interface applications
ii libcgmanager0 0.39-2ubuntu5 amd64 Central cgroup manager daemon (client library)
ii libcheese-gtk25 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam - widgets
ii libchees8 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam - base library
ii libcilkrtss5 5.4.0-6ubuntu1~16.04.11 amd64 Intel Cilk Plus language extensions (runtime)
ii libclass-accessor-perl 0.34-1 all Perl module that automatically generates accessors
ii libclone-perl 0.38-1build1 amd64 module for recursively copying Perl datatypes
ii libclucene-contribs1v5 2.3.3.4-4.1 amd64 language specific text analyzers (runtime)
ii libclucene-core1v5 2.3.3.4-4.1 amd64 core library for full-featured text search engine (runtime)
ii libclutter-1.0-0 1.24.2-1 amd64 Open GL based interactive canvas library
ii libclutter-1.0-common 1.24.2-1 all Open GL based interactive canvas library (common files)
ii libclutter-gst-3.0-0 3.0.18-1 amd64 Open GL based interactive canvas library GStreamer elements
ii libclutter-gtk-1.0-0 1.6.6-1 amd64 Open GL based interactive canvas library GTK+ widget
ii libcmis-0.5-5v5 0.5.1-Subunt2 amd64 CMIS protocol client library
ii libcogl-common 1.22.0-2 all Object oriented GL/GLES Abstraction/Utility Layer (common files)
ii libcogl-pango20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl-path20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcolamd2.9.1 1.4.4.6-1 amd64 column approximate minimum degree ordering library for sparse matrices
ii libcolord2 1.2.12-1ubuntu1 amd64 system service to manage device colour profiles -- runtime
ii libcolorhug2 1.2.12-1ubuntu1 amd64 library to access the ColorHug colourimeter -- runtime
ii libcolumbus1-common 1.1.0+15.10.20150806-0ubuntu4 all error tolerant matching engine - common files
ii libcolumbus1v5 1.1.0+15.10.20150806-0ubuntu4 amd64 error tolerant matching engine - shared library
ii libcomerr2 1.42.13-1ubuntu1 amd64 Common error description library
ii libcompizconfig0 1:0.9.12.3+16.04.20180221-0ubuntu1 amd64 Settings library for plugins - OpenCompositing Project
ii libcrack2 2.9.2-1ubuntu1 amd64 pro-active password checker library
ii libcroco3 0.6.11-1 amd64 Cascading Style Sheet (CSS) parsing and manipulation toolkit
ii libcryptsetup4 2:1.6.6-5ubuntu2.1 amd64 disk encryption support - shared library
ii libcurl3 7.47.0-1ubuntu2.12 amd64 easy-to-use client-side URL transfer library (OpenSSL flavour)
ii libcurl13-gnutls 7.47.0-1ubuntu2.12 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libdaemon0 0.14-6 amd64 lightweight C library for daemons - runtime library
ii libdata-alias-perl 1.20-1build1 amd64 module to create aliases instead of copies
ii libdatatrie1 0.2.10-2 amd64 Double-array trie library
ii libdb5.3 5.3.28-11ubuntu0.1 amd64 Berkeley v5.3 Database Libraries [runtime]
ii libdbd-mysql-perl 4.033-1ubuntu0.1 amd64 Perl5 database interface to the MySQL database
ii libdbi-perl 1.634-1build1 amd64 Perl Database Interface (DBI)
ii libdbus-1-3 1.10.6-1ubuntu3.3 amd64 simple interprocess messaging system (library)
ii libdbus-glib-1-2 0.106-1 amd64 simple interprocess messaging system (GLib-based shared library)
ii libdbusmenu-glib4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus
ii libdbusmenu-gtk3-4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus - GTK+ version
ii libdbusmenu-gtk4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus - GTK+ version
ii libdbusmenu-qt5 0.9.3+16.04.20160218-0ubuntu1 amd64 Qt implementation of the DBusMenu protocol
ii libdbusmenu-qt5 0.9.3+16.04.20160218-0ubuntu1 amd64 Qt5 implementation of the DBusMenu protocol
ii libdconf1 0.24.0-2 amd64 simple configuration storage system - runtime library
ii libdconfclient0 0.198ubuntu1 amd64 Debian Configuration Management System (C-implementation library)
ii libdecoration0 1:0.9.12.3+16.04.20180221-0ubuntu1 amd64 Compiz window decoration library
ii libdee-1.0-4 1.2.7+15.04.20150304-0ubuntu2 amd64 model to synchronize multiple instances over DBus - shared lib
ii libdevmapper1.02.1 2:1.02.110-1ubuntu10 amd64 Linux Kernel Device Mapper userspace library
ii libdfu0 0.8.3-0ubuntu1 amd64 Firmware update daemon library for DFU support
ii libdigest-hmac-perl 1.03+dfsg-1 all module for creating standard message integrity checks
ii libdjvuibre-text 3.5.27.1-5 all Linguistic support files for libdjvuibre
ii libdjvuibre21 3.5.27.1-5 amd64 Runtime support for the DjVu image format
ii libdmapsharing-3.0-2 2.9.34-1 amd64 DMAP client and server library - runtime
ii libdns-export162 1:9.10.3.dfsg.1-8ubuntu1.12 amd64 Exported DNS Shared Library
ii libdns162 1:9.10.3.dfsg.1-8ubuntu1.12 amd64 DNS Shared Library used by BIND
ii libdotconf0 1.3-0.2 amd64 Configuration file parser library - runtime files
ii libdouble-conversion1v5 2.0.1-3ubuntu2 amd64 routines to convert IEEE floats to and from strings
ii libdpkg-perl 1.18.4ubuntu1.5 all Dpkg perl modules
ii libdrm-amdgpu1 2.4.91-2~16.04.1 amd64 Userspace interface to amdgpu-specific kernel DRM services -- runtime
ii libdrm-common 2.4.91-2~16.04.1 all Userspace interface to kernel DRM services -- common files
ii libdrm-intel 2.4.91-2~16.04.1 amd64 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau2 2.4.91-2~16.04.1 amd64 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.91-2~16.04.1 amd64 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.91-2~16.04.1 amd64 Userspace interface to kernel DRM services -- runtime
ii libdv4 1.0.0-7 amd64 software library for DV format digital video (runtime lib)
ii libe-book-0.1-1 0.1.2-2ubuntu1 amd64 library for reading and converting various e-book formats
ii libebbackend-1.2-10 3.18.5-1ubuntu1.1 amd64 Utility library for evolution data servers
ii libebook-1.2-16 3.18.5-1ubuntu1.1 amd64 Client library for evolution address books
ii libebook-contacts-1.2-2 3.18.5-1ubuntu1.1 amd64 Client library for evolution contacts books
ii libecal-1.2-19 3.18.5-1ubuntu1.1 amd64 Client library for evolution calendars
ii libedata-book-1.2-25 3.18.5-1ubuntu1.1 amd64 Backend library for evolution address books
ii libedata-cal-1.2-28 3.18.5-1ubuntu1.1 amd64 Backend library for evolution calendars
ii libedataserver-1.2-21 3.18.5-1ubuntu1.1 amd64 Utility library for evolution data servers
ii libedataserverui-1.2-1 3.18.5-1ubuntu1.1 amd64 Utility library for evolution data servers
ii libedit2 3.1-20150325-1ubuntu2 amd64 BSD editline and history libraries

```

```

ii libegl11-mesa 18.0.5-0ubuntu0~16.04.1 amd64 free implementation of the EGL API -- runtime
ii libelf1 0.165-3ubuntu1.1 amd64 library to read and write ELF files
ii libemail-valid-perl 1.198-1 all Perl module for checking the validity of Internet email addresses
ii libenchant1c2a 1.6.0-10.1ubuntu2 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 libeoto 0.01-3ubuntu1 amd64 Library for parsing/converting Embedded OpenType files
ii libepoxy0 1.3.1-1ubuntu0.16.04.2 amd64 OpenGL function pointer management library
ii libespeak1 1.48.04+dfsg-2 amd64 Multi-lingual software speech synthesizer: shared library
ii libestr0 0.1.10-1 amd64 Helper functions for handling strings (lib)
ii libetonyek-0.1-1 0.1.6-1ubuntu1 amd64 library for reading and converting Apple Keynote presentations
ii libevdev2 1.4.6+dfsg-1 amd64 wrapper library for evdev devices
ii libevdocument3-4 3.18.2-1ubuntu4.3 amd64 Document (PostScript, PDF) rendering library
ii libevent-2.0-5 2.0.21-stable-2ubuntu0.16.04.1 amd64 Asynchronous event notification library
ii libevview3-3 3.18.2-1ubuntu4.3 amd64 Document (PostScript, PDF) rendering library - Gtk+ widgets
ii libexempi3 2.2.2-2ubuntu0.1 amd64 library to parse XMP metadata (Library)
ii libexif12 0.6.21-2 amd64 library to parse EXIF files
ii libexiv2-14 0.25-2.1ubuntu16.04.3 amd64 EXIF/IPTC/XMP metadata manipulation library
ii libexpat1 2.1.0-7ubuntu0.16.04.3 amd64 XML parsing C library - runtime library
ii libexporter-tiny-perl 0.042-1 all tiny exporter similar to Sub::Exporter
ii libexttextcat-2.0-0 3.4.4-1ubuntu3 amd64 Language detection library
ii libexttextcat-data 3.4.4-1ubuntu3 all Language detection library - data files
ii libfakeroot 1.20.2-1ubuntu1 amd64 tool for simulating superuser privileges - shared libraries
ii libfcgi-perl 0.77-1build1 amd64 helper module for FastCGI
ii libfcitx-config4 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - configuration support library
ii libfcitx-gclient0 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - D-Bus client library for Glib
ii libfcitx-utils0 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - utility support library
ii libfdisk1 2.27.1-6ubuntu3.6 amd64 fdisk_partitioning library
ii libffif13 3.2.1-4 amd64 Foreign Function Interface library runtime
ii libfftw3-double3 3.3.4-2ubuntu1 amd64 Library for computing Fast Fourier Transforms - Double precision
ii libfftw3-single3 3.3.4-2ubuntu1 amd64 Library for computing Fast Fourier Transforms - Single precision
ii libfile-basedir-perl 0.07-1 all Perl module to use the freedesktop basedir specification
ii libfile-copy-recursive-perl 0.38-1 all Perl extension for recursively copying files and directories
ii libfile-desktopentry-perl 0.22-1 all Perl module to handle freedesktop_desktop files
ii libfile-fcntllock-perl 0.22-3 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 0.27-1 all Perl module to determine file types
ii libflac8 1.3.1-4 amd64 Free Lossless Audio Codec - runtime C library
ii libfont-afm-perl 1.20-1 all Font::AFM - Interface to Adobe Font Metrics files
ii libfontconfig 2.11.94-0ubuntu1.1 amd64 generic font configuration library - runtime
ii libfontembed1 1.8.3-2ubuntu3.4 amd64 OpenPrinting CUPS Filters - Font Embed Shared library
ii libfontenc1 1:1.1.3-1 amd64 X11 font encoding library
ii libframe6 2.5.0daily13.06.05+16.04.20160809-0ubuntu1 amd64 Touch Frame Library
ii libfreehand-0.1-1 0.1.1-1ubuntu1 amd64 Library for parsing the FreeHand file format structure
ii libfreerdp-cache1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (cache library)
ii libfreerdp-client1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (client library)
ii libfreerdp-codec1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (codec library)
ii libfreerdp-common1.0.0 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (common library)
ii libfreerdp-core1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (core library)
ii libfreerdp-crypto1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (freerdp-crypto library)
ii libfreerdp-gdi1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (GDI library)
ii libfreerdp-locale1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (locale library)
ii libfreerdp-plugins-standard 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 RDP client for Windows Terminal Services (plugins)
ii libfreerdp-primitives1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (primitives library)
ii libfreerdp-utils1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Free Remote Desktop Protocol library (freerdp-utils library)
ii libfreetype6 2.6.1-0.1ubuntu2.3 amd64 FreeType 2 font engine, shared library files
ii libfbribidi0 0.19.7-1 amd64 Free Implementation of the Unicode BiDi algorithm
ii libfuse2 2.9.4-1ubuntu3.1 amd64 Filesystem in Userspace (library)
ii libfwup0 0.5-2ubuntu7 amd64 Library to manage UEFI firmware updates
ii libfwupd1 0.8.3-0ubuntu4 amd64 Firmware update daemon library
ii libgail-3-0 3.18.9-1ubuntu3.3 amd64 GNOME Accessibility Implementation Library -- shared libraries
ii libgail-common 2.24.30-1ubuntu1.16.04.2 amd64 GNOME Accessibility Implementation Library -- common modules
ii libgail18 2.24.30-1ubuntu1.16.04.2 amd64 GNOME Accessibility Implementation Library -- shared libraries
ii libgbm1 18.0.5-0ubuntu0~16.04.1 amd64 generic buffer management API -- runtime
ii libgc1c2 1:7.4.2-7.3ubuntu0.1 amd64 conservative garbage collector for C and C++
ii libgcap-1.0-0 0.7-1ubuntu0.1 amd64 Microsoft Cabinet file manipulation library
ii libgcc-5-dev 5.4.0-6ubuntu1~16.04.11 amd64 GCC support library (development files)
ii libgcc1 1:6.0.1-0ubuntu1 amd64 GCC support library
ii libgck-1-0 3.18.0-1ubuntu1 amd64 Glib wrapper library for PKCS#11 - runtime
ii libgconf-2-4 3.2.6-3ubuntu6 amd64 GNOME configuration database system (shared libraries)
ii libgcr-3-common 3.18.0-1ubuntu1 all Library for Crypto UI related tasks - common files
ii libgcr-base-3-1 3.18.0-1ubuntu1 amd64 Library for Crypto related tasks
ii libgcr-ui-3-1 3.18.0-1ubuntu1 amd64 Library for Crypto UI related tasks
ii libgcrypt20 1.6.5-2ubuntu0.5 amd64 LGPL Crypto Library - runtime library
ii libgd3 2.1.1-4ubuntu0.16.04.10 amd64 GD Graphics Library
ii libgdata-common 0.17.4-1 all Library for accessing GData webservices - common data files
ii libgdbm3 1.8.3-13.1 amd64 GNU dbm database routines (runtime version)
ii libgdk-pixbuf2.0-0 2.32.2-1ubuntu1.5 amd64 GDK Pixbuf library
ii libgdk-pixbuf2.0-common 2.32.2-1ubuntu1.5 all GDK Pixbuf library - data files
ii libgee-0.8-2 0.18.0-1 amd64 GObject based collection and utility library
ii libgeis1 2.2.17+16.04.20160126-0ubuntu1 amd64 Gesture engine interface support
ii libgeoclue0 0.12.99-4ubuntu1 amd64 C API for GeoClue
ii libgeocode-glib0 3.18.2-1 amd64 geocoding and reverse geocoding GLib library using Nominatim
ii libgeoip1 1.6.9-1 amd64 non-DNS IP-to-country resolver library
ii libgeonames0 0.2+16.04.20160321-0ubuntu1 amd64 Parse and query the geonames database dump
ii libgettextpo-dev 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library development files
ii libgettextpo0 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library
ii libgexiv2-2 0.10.3-2 amd64 GObject-based wrapper around the Exiv2 library
ii libgirepository-1.0-1 1.46.0-3ubuntu1 amd64 Library for handling GObject introspection data (runtime library)
ii libgl1-mesa-dri 18.0.5-0ubuntu0~16.04.1 amd64 free implementation of the OpenGL API -- DRI modules
ii libgl1-mesa-glx 18.0.5-0ubuntu0~16.04.1 amd64 free implementation of the OpenGL API -- GLX runtime
ii libglapi-mesa 18.0.5-0ubuntu0~16.04.1 amd64 free implementation of the GL API -- shared library
ii libglew1.13 1.13.0-2 amd64 OpenGL Extension Wrangler - runtime environment
ii libglewmx1.13 1.13.0-2 amd64 OpenGL Extension Wrangler (Multiple Rendering Contexts)
ii libglib-perl 3:1.320-2 amd64 Interface to the GLib and GObject libraries

```

```

ii libglib2.0-0 2.48.2-0ubuntu4.1 amd64 GLib library of C routines
ii libglib2.0-bin 2.48.2-0ubuntu4.1 amd64 Programs for the GLib library
ii libglibmm-2.4-1v5 2.46.3-1 amd64 C++ wrapper for the GLib toolkit (shared libraries)
ii libglu1-mesa 9.0.0-2.1 amd64 Mesa OpenGL utility library (GLU)
ii libgnome-2.6-0 2.6.20-1 amd64 MIME message parser and creator library - runtime
ii libgmp10 2;6.1.0+dfsg-2 amd64 Multiprecision arithmetic library
ii libgnome-bluetooth3 3.18.2-1ubuntu2 amd64 GNOME Bluetooth tools - support library
ii libgnome-desktop-3-12 3.18.2-1ubuntu1 amd64 Utility library for loading .desktop files - runtime files
ii libgnome-keyring-common 3.12.0-1build1 all GNOME keyring services library - data files
ii libgnome-keyring0 3.12.0-1build1 amd64 GNOME keyring services library
ii libgnome-menu-3-0 3.13.3-6ubuntu3.1 amd64 GNOME implementation of the freedesktop menu specification
ii libgnomekbd-common 3.6.0-1ubuntu2 all GNOME library to manage keyboard configuration - common files
ii libgnomekbd8 3.6.0-1ubuntu2 amd64 GNOME library to manage keyboard configuration - shared library
ii libgnutls-openssl27 3.4.10-4ubuntu1.4 amd64 GNU TLS library - OpenSSL wrapper
ii libgnutls30 3.4.10-4ubuntu1.4 amd64 GNU TLS library - main runtime library
ii libgoa-1.0-0b 3.18.3-1ubuntu2 amd64 library for GNOME Online Accounts
ii libgoa-1.0-common 3.18.3-1ubuntu2 all library for GNOME Online Accounts - common files
ii libgom-1.0-0 0.3.1-1 amd64 Object mapper from GObjects to SQLite
ii libgom-1.0-common 0.3.1-1 all libgom architecture-independent files
ii libgomp1 5.4.0-6ubuntu1~16.04.11 amd64 GCC_OpenMP (GOMP) support library
ii libgpg-error0 1.21-2ubuntu1 amd64 library for common error values and messages in GnuPG components
ii libgpgme11 1.6.0-1 amd64 GPGME - GnuPG Made Easy (library)
ii libgphoto2-0 2.5.9-3 amd64 gphoto2 digital camera library
ii libgphoto2-110n 2.5.9-3 all gphoto2 digital.camera library - localized messages
ii libgphoto2-port12 2.5.9-3 amd64 gphoto2 digital.camera port library
ii libgpml2 1.20.4-6.1 amd64 General Purpose Mouse - shared library
ii libgpod-common 0.8.3-6ubuntu2 amd64 common files for libgpod
ii libgpod4 0.8.3-6ubuntu2 amd64 library to read and write songs and artwork to an iPod
ii libgrail6 3.1.0+16.04.20160125-0ubuntu1 amd64 Gesture Recognition And Instantiation Library
ii libgraphite2-3 1.3.10-0ubuntu0.16.04.1 amd64 Font rendering engine for Complex Scripts -- library
ii libgrilo-0.2-1 0.2.15-1 amd64 Framework for discovering and browsing media - Shared libraries
ii libgs9 9.26~dfsg+0~ubuntu0.16.04.7 amd64 interpreter for the PostScript language and for PDF - Library
ii libgs9-common 9.26~dfsg+0~ubuntu0.16.04.7 all interpreter for the PostScript language and for PDF - common files
ii libgsettings-gt1 0.1+16.04.20160329-0ubuntu1 amd64 Library to access GSettings from Qt
ii libgssapi-krb5-2 1.13.2+dfsg-5ubuntu2.1 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssapi3-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - GSSAPI support library
ii libgstreamer-plugins-base1.0-0 1.8.3-1ubuntu0.2 amd64 GStreamer libraries from the "base" set
ii libgstreamer-plugins-good1.0-0 1.8.3-1ubuntu0.4 amd64 GStreamer development files for libraries from the "good" set
ii libgstreamer1.0-0 1.8.3-1ubuntu0.1 amd64 Core GStreamer libraries and elements
ii libgtk-3-0 3.18.9-1ubuntu3.3 amd64 GTK+ graphical user interface library
ii libgtk-3-bin 3.18.9-1ubuntu3.3 amd64 programs for the GTK+ graphical user interface library
ii libgtk-3-common 3.18.9-1ubuntu3.3 all common files for the GTK+ graphical user interface library
ii libgtk2-perl 2:1.2498-1 amd64 Perl interface to the 2.x series of the Gimp Toolkit library
ii libgtk2.0-0.2 2.24.30-1ubuntu1.16.04.2 amd64 GTK+ graphical user interface library
ii libgtk2.0-bin 2.24.30-1ubuntu1.16.04.2 amd64 programs for the GTK+ graphical user interface library
ii libgtk2.0-common 2.24.30-1ubuntu1.16.04.2 all common files for the GTK+ graphical user interface library
ii libgtkmm-3.0-1v5 3.18.0-1 amd64 C++ wrappers for GTK+ (shared libraries)
ii libgtksourceview-3.0-1 3.18.2-1 amd64 shared libraries for the GTK+ syntax highlighting widget
ii libgtksourceview-3.0-common 3.18.2-1 all common files for the GTK+ syntax highlighting widget
ii libgtkspell3-3-0 3.0.7-2 amd64 spell-checking addon for GTK+'s TextView widget
ii libgtop-2.0-10 2.32.0-1 amd64 gtop system monitoring library (shared)
ii libgtop2-common 2.32.0-1 all gtop system monitoring library (common)
ii libgucharmap-2-90-7 1:3.18.2-1ubuntu1 amd64 Unicode browser widget library (shared library)
ii libgudev-1.0-0 1:230-2 amd64 GObject-based wrapper library for libudev
ii libgusb2 0.2.9-0ubuntu1 amd64 GLib wrapper around libusb1
ii libgutenprint2.5.2.11-1 amd64 runtime for the Gutenprint printer driver library
ii libgweather-3-6 3.18.2-0ubuntu0.2 amd64 GWeather shared library
ii libgweather-common 3.18.2-0ubuntu0.2 all GWeather common files
ii libgxps2 0.2.3.2-1 amd64 handling and rendering XPS documents (library)
ii libhardware2 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Library to provide access to the Android libhardware HAL
ii libharfbuzz-icu0 1.0.1-1ubuntu0.1 amd64 OpenType text shaping engine ICU backend
ii libharfbuzz0b 1.0.1-1ubuntu0.1 amd64 OpenType text shaping engine (shared library)
ii libhcrypt04-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - crypto library
ii libheimbase1-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - Base library
ii libheimntlm0-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - NTLM support library
ii libhogweed4 3.2-1ubuntu0.16.04.1 amd64 low level cryptographic library (public-key_cryptos)
ii libhpmd0 3.16.3+repack0-1 amd64 HP Multi-Point Transport Driver (hpmd) run-time libraries
ii libhtml-form-perl 6.03-1 all module that represents an HTML form element
ii libhtml-format-perl 2.11-2 all module for transforming HTML into various formats
ii libhtml-parser-perl 3.72-1 amd64 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-2 all Data tables pertaining to HTML
ii libhtml-template-perl 2.95-2 all module for using HTML templates with Perl
ii libhtml-tree-perl 5.03-2 all Perl module to represent and create HTML syntax trees
ii libhttp-cookies-perl 6.01-1 all HTTP cookie jars
ii libhttp-daemon-perl 6.01-1 all simple http server class
ii libhttp-date-perl 6.02-1 all module of date conversion routines
ii libhttp-message-perl 6.11-1 all perl interface to HTTP style messages
ii libhttp-negotiate-perl 6.00-2 all implementation of content negotiation
ii libhud2 14:10+16.04.20160415-0ubuntu1 amd64 library for exporting items to the Unity HUD
ii libhunspell-1.3-0 1.3.3-4ubuntu1 amd64 spell checker and morphological analyzer (shared library)
ii libhx509-5-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - X509 support library
ii libhybris 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Allows to run bionic-based HW adaptations in glibc systems - libs
ii libhybris-common1 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Common library that contains the Android linker and custom hooks
ii libhyphen0 2.8.8-2ubuntu1 amd64 ALTLinux hyphenation library - shared library
ii libibus-1.0-5 1.5.11-1ubuntu2.1 amd64 Intelligent Input Bus - shared library
ii libical1a 1.0.1-0ubuntu2 amd64 iCalendar library implementation in C (runtime)
ii libice6 2:1.0.9-1 amd64 X11 Inter-Client Exchange library
ii libicu55 55.1-7ubuntu0.4 amd64 International Components for Unicode
ii libicu65 65.1-1+ubuntu16.04.1+deb.sury.org+1 amd64 International Components for Unicode
ii libidn11 1.32-3ubuntu1.2 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libidn03-0.1-0 13.10.0-16.04.04.20161028-0ubuntu1 amd64 Shared library providing extra gtk menu items for display in
ii libiec61883-0 1.2.0-0.2 amd64 an partial implementation of IEC 61883
ii libieee1284-3 0.2.11-12 amd64 cross-platform library for parallel port access
ii libijs-0.35 0.35-12 amd64 IJS raster image transport protocol: shared library
ii libilmbase12 2.2.0-11ubuntu2 amd64 several utility libraries from ILM used by OpenEXR
ii libimobiledevice6 1.2.0+dfsg-3~ubuntu0.2 amd64 Library for communicating with the iPhone and iPod Touch
ii libindicator3-7 12.10.2+16.04.20151208-0ubuntu1 amd64 panel indicator applet - shared library
ii libinput-bin 1.6.3-1ubuntu1~16.04.1 amd64 input device management and event handling library - udev quirks

```

```

ii libinput10 1:6.3-1ubuntu1~16.04.1 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-pty-perl 1:1.08-1.1build1 amd64 Perl module for pseudo tty IO
ii libio-socket-inet6-perl 2.72-2 all object interface for AF_INET6 domain sockets
ii libio-socket-ssl-perl 2.024-1 all Perl module implementing object oriented interface to SSL sockets
ii libio-string-perl 1.08-3 all Emulate IO::File interface for in-core strings
ii libipc-run-perl 0.94-1 all Perl module for running processes
ii libipc-system-simple-perl 1.25-3 all Perl module to run commands simply, with detailed diagnostics
ii libisc-export160 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 Exported ISC Shared Library
ii libisc160 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 ISC Shared Library used by BIND
ii libisccc140 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 Command Channel Library used by BIND
ii libiscfg140 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 Config File Handling Library used by BIND
ii libis115 0.16.1-1 amd64 manipulating sets and relations of integer points bounded by linear constraints
ii libitm1 5.4.0-6ubuntu1~16.04.11 amd64 GNU Transactional Memory Library
ii libiw30 30~pre9-8ubuntu1 amd64 Wireless tools - library
ii libjack-jackd2-0 1.9.10+20150825git50c92-dfsg-1 amd64 JACK Audio Connection Kit (libraries)
ii libjasper1.1.900.1-debian1-2.4ubuntu1.2 amd64 JasPer JPEG-2000 runtime library
ii libjavascripcoregtk-4.0-18 2.20.5~0ubuntu0.16.04.1 amd64 JavaScript engine library from WebKitGTK+
ii libjbig0 2.1-3.1 amd64 JBIGkit libraries
ii libjbig2dec0 0.12+20150918-1ubuntu0.1 amd64 JBIG2 decoder library - shared libraries
ii libjpeg-turbo8 1.4.2-0ubuntu1.1 amd64 IJG JPEG compliant runtime library.
ii libjpeg8 8c-2ubuntu8 amd64 Independent JPEG Group's JPEG runtime library (dependency package)
ii libjson-c2_0.11-4ubuntu2 amd64 JSON manipulation library - shared library
ii libjson-glib-1.0-0 1.1.2-0ubuntu1 amd64 GLib JSON manipulation library
ii libjson-glib-1.0-common 1.1.2-0ubuntu1 all GLib JSON manipulation library (common files)
ii libkrb5crypto3 1.13.2+dfsg-5ubuntu2.1 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.9-8ubuntu1 amd64 Linux Key Management Utilities (library)
ii libklibc 2.0.4-8ubuntu1.16.04.4 amd64 minimal libc subset for use with initramfs
ii libkmod2 22-1ubuntu5.2 amd64 libkmod shared library
ii libkpathsea0 2015.20160222.37495-1ubuntu1.1 amd64 TeX Live: path search library for TeX (runtime part)
ii libkrb5-26-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - libraries
ii libkrb5-3 1.13.2+dfsg-5ubuntu2.1 amd64 MIT Kerberos runtime libraries
ii libkrb5support0 1.13.2+dfsg-5ubuntu2.1 amd64 MIT Kerberos runtime libraries - Support library
ii libksbsa8 1.3.3-1ubuntu0.16.04.1 amd64 X.509 and CMS support library
ii liblangtag-common 0.5.7-2ubuntu1 all library to access tags for identifying languages -- data
ii liblangtag1 0.5.7-2ubuntu1 amd64 library to access tags for identifying languages
ii liblcms2-2_2.6-3ubuntu2.1 amd64 Little CMS 2 color management library
ii liblcms2-utils 2.6-3ubuntu2.1 amd64 Little CMS 2 color management library (utilities)
ii libldap-2.4-2 2.4.42+dfsg-2ubuntu3.4 amd64 OpenLDAP libraries
ii libldbc 2.1:1.24-1ubuntu3.1 amd64 LDAP-like embedded database - shared library
ii liblightdm-gobject-1-0 1.18.3-0ubuntu1.1 amd64 LightDM GObject client library
ii liblircclient0 0.9.0-0ubuntu6 amd64 infra-red remote control support - client library
ii liblist-moreutils-perl 0.413-1build1 amd64 Perl module with additional list functions not found in List::Util
ii libl1vms3.8 1:3.8-2ubuntu4 amd64 Modular compiler and toolchain technologies, runtime library
ii libl1vms6.0 1:6.0-1ubuntu2~16.04.1 amd64 Modular compiler and toolchain technologies, runtime library
ii liblocale-gettext-perl 1.07-1build1 amd64 module using libc functions for internationalization in Perl
ii liblouis-data 2.6.4-2ubuntu0.4 all Braille translation library - data
ii liblouis9 2.6.4-2ubuntu0.4 amd64 Braille translation library - shared libs
ii liblouisutdml-bin 2.5.0-3 amd64 Braille UTDML translation utilities
ii liblouisutdml-data 2.5.0-3 all Braille UTDML translation library - data
ii liblouisutdml16 2.5.0-3 amd64 Braille UTDML translation library - shared libs
ii liblqr-1-0 0.4.2-2 amd64 converts plain array images into multi-size representation
ii liblsan0 5.4.0-6ubuntu1~16.04.11 amd64 LeakSanitizer -- a memory leak detector (runtime)
ii libltdl7 2.4.6-0.1 amd64 System independent dlopen wrapper for GNU libtool
ii libluas5.1-0 5.1.5-8ubuntu1 amd64 Shared library for the Lua interpreter version 5.1
ii libluas5.2-0 5.2.4-1ubuntu1 amd64 Shared library for the Lua interpreter version 5.2
ii liblwp-mediatypes-perl 6.02-1 all module to guess media type for a file or a URL
ii liblwp-protocol-https-perl 6.06-2 all HTTPS driver for LWP::UserAgent
ii liblwres141 1:9.10.3.dfsg.P4-8ubuntu1.12 amd64 Lightweight Resolver Library used by BIND
ii liblz4-1 0.0~r131~2ubuntu2 amd64 Fast LZ compression algorithm library - runtime
ii liblzma5 5.1.1alpha20120614-2ubuntu2 amd64 XZ-format compression library
ii liblzoz2-2 2.08-1.2 amd64 data compression library
ii libmagic1 1:5.25-2ubuntu1.1 amd64 File type determination library using "magic" numbers
ii libmagickcore-6.q16-2 8:6.8.9.9-7ubuntu5.13 amd64 low-level image manipulation library -- quantum depth Q16
ii libmagickcore-6.q16-2-extra 8:6.8.9.9-7ubuntu5.13 amd64 low-level image manipulation library - extra codecs (Q16)
ii libmagickwand-6.q16-2 8:6.8.9.9-7ubuntu5.13 amd64 image manipulation library
ii libmailtools-perl 2.13-1 all Manipulate email in perl programs
ii libmbim-glib4 1.14.0-1ubuntu0.16.04.1 amd64 Support library to use the MBIM protocol
ii libmbim-proxy 1.14.0-1ubuntu0.16.04.1 amd64 Proxy to communicate with MBIM ports
ii libmedial 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Library to provide access to the Android Media HAL
ii libmediaart-2.0-0 1.9.0-2 amd64 media art extraction and cache management library
ii libmessaging-menu0 13.10.1+15.10.20150505-0ubuntu1 amd64 Messaging Menu - shared library
ii libmetacity-private3a 1:3.18.7-0ubuntu0.3 amd64 library for the Metacity window manager
ii libmhash2 0.9.9.9-7 amd64 Library for cryptographic hashing and message authentication
ii libminiuunpnc10 1:9.20140610-2ubuntu2.16.04.2 amd64 UPnP IGD client lightweight library
ii libmircclient9 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - client library
ii libmircommon5 0.21.0+16.04.20160330-0ubuntu1 amd64 Display server for Ubuntu - shared library
ii libmircommon7 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - shared library
ii libmircore1 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - shared library
ii libmirprotobuf3 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - RPC definitions
ii libmm-glib0 1:6.4-1ubuntu0.16.04.1 amd64 D-Bus service for managing modems - shared libraries
ii libmng2 2.0.2-0ubuntu3 amd64 Multiple-image Network Graphics library
ii libmn10 1.0.3-5 amd64 minimalistic Netlink communication library
ii libmount1 2.27.1-6ubuntu3.6 amd64 device mounting library
ii libmpc3 1.0.3-1 amd64 multiple precision complex floating-point library
ii libmpdec2 2.4.2-1 amd64 library for decimal floating point arithmetic (runtime library)
ii libmpfr4 3.1.4-1 amd64 multiple precision floating-point computation
ii libmpx0 5.4.0-6ubuntu1~16.04.11 amd64 Intel memory protection extensions (runtime)
ii libmspub-0.1-1.0.1.2-2ubuntu1 amd64 library for parsing the mspub file structure
ii libmtdev1 1.1.5-1ubuntu2 amd64 Multitouch Protocol Translation Library - shared library
ii libmtp-common 1.1.10-2ubuntu1 all Media Transfer Protocol (MTP) common files
ii libmtp-runtime 1.1.10-2ubuntu1 amd64 Media Transfer Protocol (MTP) runtime tools
ii libmtp9 1.1.10-2ubuntu1 amd64 Media Transfer Protocol (MTP) library
ii libmwaw-0.3-3 0.3.7-1ubuntu2.1 amd64 import library for some old Mac text documents
ii libmysqlclient20 5.7.30-0ubuntu0.16.04.1 amd64 MySQL database client library
ii libmythes-1.2-0 2:1.2.4-1ubuntu3 amd64 simple thesaurus library
ii libnatpmp1 20110808-4 amd64 portable and fully compliant implementation of NAT-PMP
ii libnautilus-extension1a 1:3.18.4.1-3.14.3-0ubuntu6 amd64 libraries for nautilus components - runtime version
ii libncurses5 6.0+20160213-1ubuntu1 amd64 shared libraries for terminal handling

```

```

ii libncursesw5 6.0+20160213-1ubuntu1 amd64 shared libraries for terminal handling (wide character support)
ii libndp0 1.4-2ubuntu0.16.04.1 amd64 Library for Neighbor Discovery Protocol
ii libneon27-gnutls 0.30.1-3build1 amd64 HTTP and WebDAV client library (GnuTLS enabled)
ii libnet-dbus-perl 1.1.0-3build1 amd64 Perl extension for the DBus bindings
ii libnet-dns-perl 0.81-2build1 amd64 Perform DNS queries from a Perl script
ii libnet-domain-tld-perl 1.73-1 all list of currently available Top-level Domains (TLDs)
ii libnet-http-perl 6.09-1 all module providing low-level HTTP connection client
ii libnet-ip-perl 1.26-1 all Perl extension for manipulating IPv4/IPv6 addresses
ii libnet-libdn-perl 0.12.ds2build2 amd64 Perl bindings for GNU Libdn
ii libnet-smtp-perl 1.03-1 all Perl module providing SSL support to Net::SMTP
ii libnet-ssleay-perl 1.72-1build1 amd64 Perl module for Secure Sockets Layer (SSL)
ii libnetfilter-contrack3 1.0.5-1 amd64 Netfilter netlink-contrack library
ii libnetpbm10 2:10.0-15.3 amd64 Graphics conversion tools shared libraries
ii libnettle6 3.2-1ubuntu0.16.04.1 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52-18-1ubuntu2 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnftnlk0 1.0.1-3 amd64 Netfilter netlink library
ii libnih-dbus1 1.0.3-4.3ubuntu1 amd64 NIH D-Bus Bindings Library
ii libnih1 1.0.3-4.3ubuntu1 amd64 NIH Utility Library
ii libnl3-200 3.2.27-1ubuntu0.16.04.1 amd64 library for dealing with netlink sockets
ii libnl-genl-3-200 3.2.27-1ubuntu0.16.04.1 amd64 library for dealing with netlink sockets - generic netlink
ii libnm-glib-vpn1 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (GLib VPN shared library)
ii libnm-glib4 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (GLib shared library)
ii libnm-gtk-common 1.2.6-0ubuntu0.16.04.4 all library for wireless and mobile dialogs - common files
ii libnm-gtk0 1.2.6-0ubuntu0.16.04.4 amd64 library for wireless and mobile dialogs (libnm-glib version)
ii libnm-util2 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (shared library)
ii libnotify0 1.2.6-0ubuntu0.16.04.4 amd64 GObject-based client library for NetworkManager
ii libnma-common 1.2.6-0ubuntu0.16.04.4 all library for wireless and mobile dialogs - common files
ii libnotify-bin 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon (Utilities)
ii libnotify4 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon
ii libnpth0 1.2.3 amd64 replacement for GNU Pth using system threads
ii libnspr4 2:4.13.1-0ubuntu0.16.04.1 amd64 NetScape Portable Runtime Library
ii libnss-mdns 0.10-7 amd64 NSS module for Multicast DNS name resolution
ii libnss3 2:3.28.4-0ubuntu0.16.04.4 amd64 Network Security Service libraries
ii libnss3-nssdb 2:3.28.4-0ubuntu0.16.04.4 all Network Security Security libraries - shared databases
ii libnuma1 2.0.11-1ubuntu1.1 amd64 Libraries for controlling NUMA policy
ii libnux-4.0-0 4.0.8+16.04.20180622.2-0ubuntu1 amd64 Visual rendering toolkit for real-time applications - shared lib
ii libnux-4.0-common 4.0.8+16.04.20180622.2-0ubuntu1 all Visual rendering toolkit for real-time applications - common files
ii liboauth0 1.0.3-0ubuntu2 amd64 C library for implementing OAuth 1.0
ii libodfgen-0.1-1 0.1.6-1ubuntu2 amd64 library to generate ODF documents
ii libogg0 1.3.2-1 amd64 Ogg bitstream library
ii libopenexr22 2.2.0-10ubuntu2 amd64 runtime files for the OpenEXR image library
ii libopus0 1.1.2-1ubuntu1 amd64 Opus codec runtime library
ii liborc-0.4-0 1:0.4.25-1 amd64 Library of Optimized Inner Loops Runtime Compiler
ii liborcus-0.10-0v5 0.9.2-4ubuntu2 amd64 library for processing spreadsheet documents
ii liboxideqt-qmlplugin 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (QML plugin)
ii liboxideqtcore0 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (core library and components)
ii liboxideqtquick0 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (QtQuick library)
ii libp11-kit-gnome-keyring 3.18.3-0ubuntu2.1 amd64 GNOME keyring module for the PKCS#11 module loading library
ii libp11-kit0 0.23-2~5~ubuntu16.04.1 amd64 library for loading and coordinating access to PKCS#11 modules - runtime
ii libpackagekit-glib2-16 0.8.17-4ubuntu6~gc5.4ubuntu1.4 amd64 Library for accessing PackageKit using GLib
ii libpagemaker-0.0-0 0.0.3-1ubuntu1 amd64 Library for importing and converting PageMaker Documents
ii libpam-gnome-keyring 3.18.3-0ubuntu2.1 amd64 PAM module to unlock the GNOME keyring upon login
ii libpam-modules 1.1.8-3.2ubuntu2.1 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.8-3.2ubuntu2.1 all Runtime support for the PAM library
ii libpam-systemd 229-4ubuntu21.16 amd64 system and service manager - PAM module
ii libpam0g 1.1.8-3.2ubuntu2.1 amd64 Pluggable Authentication Modules library
ii libpango-0.1.0-1 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpango-perl 1.227-1 amd64 Perl module to layout and render internationalized text
ii libpango1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text (transitional package)
ii libpangocairo-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpangoft2-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpangomm-1.4-1v5 2.38.1-1 amd64 C++ Wrapper for pango (shared libraries)
ii libpangoox-1.0-0 0.0.2-5 amd64 pango library X backend
ii libpangooxft-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpaper-utils 1.1.24+nmu4ubuntu1 amd64 library for handling paper characteristics (utilities)
ii libpaper1 1.1.24+nmu4ubuntu1 amd64 library for handling paper characteristics
ii libparse-debianchangelog-perl 1.2.0-8 all parse Debian changelogs and output them in other formats
ii libparted2 3.2-15ubuntu0.1 amd64 disk partition manipulator - shared library
ii libpcap0.8 1.7.4-2 amd64 system interface for user-level packet capture
ii libpcp13 1:3.3.1-1ubuntu1.3 amd64 Linux PCI Utilities (shared library)
ii libpciaccess0 0.13.4-1 amd64 Generic PCI access library for X
ii libpcre16-3 2:8.38-3.1 amd64 Perl 5 Compatible Regular Expression Library - 16 bit runtime files
ii libpcre3 2:8.44-1+ubuntu16.04.1+deb.sury.org+1 amd64 Perl 5 Compatible Regular Expression Library - runtime files
ii libpcssclite1 1.8.14-1ubuntu1.16.04.1 amd64 Middleware to access a smart card using PC/SC (library)
ii libpeas-1.0-0 1.16.0-1ubuntu2 amd64 Application plugin library
ii libpeas-1.0-0-pyhton3loader 1.16.0-1ubuntu2 amd64 Application plugin library (common files)
ii libpeas-common 1.16.0-1ubuntu2 all Application plugin library (common files)
ii libperll5.22 5.22.1-9ubuntu0.6 amd64 shared Perl library
ii libperlio-gzip-perl 0.19-1build1 amd64 module providing a PerlIO layer to gzip/gunzip
ii libpipeline1 1.4.1-2 amd64 pipeline manipulation library
ii libpixman-1-0 0.33.6-1 amd64 pixel-manipulation library for X and cairo
ii libplist3 1.12-3.1ubuntu0.16.04.1 amd64 Library for handling Apple binary and XML property lists
ii libplymouth4 0.9.2-3ubuntu13.5 amd64 graphical boot animation and logger - shared libraries
ii libpng12-0 1.2.54-1ubuntu1.1 amd64 PNG library - runtime
ii libpolkit-agent-1-0 0.105-14.1ubuntu0.4 amd64 PolicyKit Authentication Agent API
ii libpolkit-backend-1-0 0.105-14.1ubuntu0.4 amd64 PolicyKit backend API
ii libpolkit-gobject-1-0 0.105-14.1ubuntu0.4 amd64 PolicyKit Authorization API
ii libpoppler-glib8 0.41.0-0ubuntu1.12 amd64 PDF rendering library (GLib-based shared library)
ii libpoppler58 0.41.0-0ubuntu1.12 amd64 PDF rendering library
ii libpopt0 1.16-10 amd64 lib for parsing cmdline parameters
ii libportaudio2 19+svn20140130-1build1 amd64 Portable audio I/O - shared library
ii libprocps4 2:3.3.10-4ubuntu2.4 amd64 library for accessing process information from /proc
ii libprotobuf-lite9v5 2.6.1-1.3 amd64 protocol buffers C++ library (lite version)
ii libproxy0 0.4.11-5ubuntu1 amd64 automatic proxy configuration management library (GSettings plugin)
ii libproxy1-plugin-networkmanager 0.4.11-5ubuntu1 amd64 automatic proxy configuration management library (Network Manager plugin)
ii libproxy1v5 0.4.11-5ubuntu1 amd64 automatic proxy configuration management library (shared)

```

```

ii libpulse-mainloop-glib0 1:8.0-0ubuntu3.10 amd64 PulseAudio client libraries (glib support)
ii libpulse0 1:8.0-0ubuntu3.10 amd64 PulseAudio client libraries
ii libpulsesdsp 1:8.0-0ubuntu3.10 amd64 PulseAudio OSS pre-load library
ii libpwpquality-common 1.3.0-0ubuntu1 all library for password quality checking and generation (data files)
ii libpwpquality1 1.3.0-0ubuntu1 amd64 library for password quality checking and generation
ii libpython-stdlib 2.7.12-1~16.04 amd64 interactive high-level object-oriented language (default python version)
ii libpython2.7 2.7.12-1ubuntu0~16.04.4 amd64 Shared Python runtime library (version 2.7)
ii libpython2.7-stdlib 2.7.12-1ubuntu0~16.04.4 amd64 Minimal subset of the Python language (version 2.7)
ii libpython2.7-stdlib 2.7.12-1ubuntu0~16.04.4 amd64 Interactive high-level object-oriented language (standard library, version 2.7)
ii libpython3-stdlib 3.5.5.1-3 amd64 interactive high-level object-oriented language (default python3 version)
ii libpython3.5 3.5.5.2-2ubuntu0~16.04.5 amd64 Shared Python runtime library (version 3.5)
ii libpython3.5-minimal 3.5.5.2-2ubuntu0~16.04.5 amd64 Minimal subset of the Python language (version 3.5)
ii libpython3.5-stdlib 3.5.5.2-2ubuntu0~16.04.5 amd64 Interactive high-level object-oriented language (standard library, version 3.5)
ii libqmi-glib1 1.12.6-1 amd64 Support library to use the Qualcomm MSM Interface (QMI) protocol
ii libqmi-glib5 1.16.2-1ubuntu0~16.04.1 amd64 Support library to use the Qualcomm MSM Interface (QMI) protocol
ii libqpdf17 6.0.0-2 amd64 runtime library for PDF transformation/inspection software
ii libqpdf21 8.0.2-3~16.04.1 amd64 runtime library for PDF transformation/inspection software
ii libqqwing2v5 1.3.4-1 amd64 tool for generating and solving Sudoku puzzles (library)
ii libqt4-dbus 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus module
ii libqt4-declarative 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 Declarative module
ii libqt4-network 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 network module
ii libqt4-script 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 script module
ii libqt4-sql 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 SQL module
ii libqt4-sql-sqlite 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 SQLite 3 database driver
ii libqt4-xml 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 XML module
ii libqt4-xmlpatterns 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 XML patterns module
ii libqt5core5a 5.5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 core module
ii libqt5dbus5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 D-Bus module
ii libqt5feedback5 5.0~git20130529-0ubuntu13 amd64 Qt Feedback module
ii libqt5gui5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 GUI module
ii libqt5multimedia5 5.5.5.1-4ubuntu2 amd64 Qt 5 Multimedia module
ii libqt5network5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 network module
ii libqt5opengl5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 OpenGL module
ii libqt5organizer5 5.0~git20140515-29475884-0ubuntu20 amd64 Qt PIM module, Organizer library
ii libqt5positioning5 5.5.1-3ubuntu1 amd64 Qt Positioning module
ii libqt5printsupport5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 print support module
ii libqt5sql5 5.5.1-2ubuntu6 amd64 Qt 5 QML module
ii libqt5quick5 5.5.1-2ubuntu6 amd64 Qt 5 Quick library
ii libqt5quicktest5 5.5.1-2ubuntu6 amd64 Qt 5 Quick Test library
ii libqt5sql5 5.5.1+dfsg-2ubuntu1 amd64 Web content engine library for Qt
ii libqt5widgets5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 widgets module
ii libqt5xml5 5.5.1+dfsg-16ubuntu7.5 amd64 Qt 5 XML module
ii libqt5dbus4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 core module
ii libqt5dbus4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus module library
ii libqt5gui4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 GUI module
ii libquadmath0 5.4.0-6ubuntu1~16.04.11 amd64 GCC Quad-Precision Math Library
ii libquvi-scripts 0.4.21-2 all library for parsing video download links (Lua scripts)
ii libquvi1 0.4.1-3 amd64 library for parsing video download links (runtime libraries)
ii libraptor2-0 2.0.14-1 amd64 Raptor 2 RDF syntax library
ii librarsql3 0.9.32-1 amd64 Rasql RDF query library
ii libraw1394-11 2.1.1-2 amd64 library for direct access to IEEE 1394 bus (aka FireWire)
ii libraw15 0.17.1-1ubuntu0.4 amd64 raw image decoder library
ii librdfl0 1.0.17-1build1 amd64 Redland Resource Description Framework (RDF) library
ii libreadline5 5.2+dfsg-3build1 amd64 GNU readline and history libraries, run-time libraries
ii libreadline6 6.3-8ubuntu2 amd64 GNU readline and history libraries, run-time libraries
ii libreoffice-avmedia-backend-gstreamer 1:5.1.6~rc2-0ubuntu1-xenial6 amd64 GStreamer backend for LibreOffice
ii libreoffice-base-core 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- shared library
ii libreoffice-calc 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- spreadsheet
ii libreoffice-common 1:5.1.6~rc2-0ubuntu1~xenial6 all office productivity suite -- arch-independent files
ii libreoffice-core 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- arch-dependent files
ii libreoffice-draw 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- drawing
ii libreoffice-gnome 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- GNOME integration
ii libreoffice-gtk 1:5.1.6~rc2-0ubuntu1-xenial6 amd64 office productivity suite -- GTK+ integration
ii libreoffice-help-en-us 1:5.1.4-0ubuntu1 all office productivity suite -- English_american help
ii libreoffice-impress 1:5.1.6~rc2-0ubuntu1-xenial6 amd64 office productivity suite -- presentation
ii libreoffice-math 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- equation editor
ii libreoffice-ogltrans 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 LibreOffice Impress extension for slide transitions using OpenGL
ii libreoffice-pdfimport 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 PDF Import component for LibreOffice
ii libreoffice-style-breeze 1:5.1.6~rc2-0ubuntu1~xenial6 all office productivity suite -- Breeze symbol style
ii libreoffice-style-galaxy 1:5.1.6~rc2-0ubuntu1~xenial6 all office productivity suite -- Galaxy (Default) symbol style
ii libreoffice-writer 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 office productivity suite -- word processor
ii librest-0.7.0 0.7.93-1 amd64 REST service access library
ii libreveng-0.0.0 0.0.4-4ubuntu1 amd64 Base Library for writing document interface filters
ii librhythmbox-core9 3.3-1ubuntu7 amd64 support library for the rhythmbox music player
ii libroken1-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - roken support library
ii librsvg2-2 2.40.13-3 amd64 SAX-based renderer library for SVG files (runtime)
ii librsvg2-common 2.40.13-3 amd64 SAX-based renderer library for SVG files (extra runtime)
ii librtmp1 2.4+20151223.gitfa8646d-1ubuntu0.1 amd64 toolkit for RTMP streams (shared library)
ii libsamplel0 0.1.8-8 amd64 Audio sample rate conversion library
ii lib sane 1.0.25+git20150528-1ubuntu2.16.04.1 amd64 API library for scanners
ii lib sane-hpao 3.16.3+repack0-1 amd64 HP SANE backend for multi-function peripherals
ii lib sasl2-2 2.1.26.dfsg1-14ubuntu0.1 amd64 Cyrus SASL - authentication abstraction library
ii lib sasl2-modules 2.1.26.dfsg1-14ubuntu0.1 amd64 Cyrus SASL - pluggable authentication modules
ii lib sasl2-modules-db 2.1.26.dfsg1-14ubuntu0.1 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii lib sasl2 1.3-1 amd64 Sub Band CODEC library - runtime
ii lib seccomp2 2.3.1-2.1ubuntu2-16.04.1 amd64 high level interface to Linux seccomp filter
ii lib secret-1-0 0.18.4-1ubuntu2 all Secret store (common files)
ii lib selinux1 2.4-3build2 amd64 SELinux runtime shared libraries
ii lib semanage-common 2.3-1build3 all Common files for SELinux policy management libraries
ii lib semanage1 2.3-1build3 amd64 SELinux policy management library
ii lib sensors4 1:3.4.9-2 amd64 library to read temperature/voltage/fan sensors
ii lib sepol1 2.4-2 amd64 SELinux library for manipulating binary security policies

```

```

ii libsgutils2-2 1.40-0ubuntu1 amd64 utilities for devices using the SCSI command set (shared libraries)
ii libshout3 2.3.1-3 amd64 MP3/Ogg Vorbis broadcast streaming library
ii libsigc++-2.0-0v5 2.6.2-1 amd64 type-safe Signal Framework for C++ - runtime
ii libsignon-extension1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libsignon-glib1 1.13+16.04.20151209.1-0ubuntu1 amd64 library for signond
ii libsignon-plugins-common1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libsignon-qt5-1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libsslang2 2.3.0-2ubuntu1.1 amd64 S-Lang programming library - runtime version
ii libsm6 2:1.2.2-1 amd64 X11 Session Management library
ii libsmartcols1 2.27.1-6ubuntu3.6 amd64 smart column output alignment library
ii lib smbclient 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 shared library for communication with SMB/CIFS servers
ii libsnappy-glib1 1.33-0ubuntu0.16.04.1 amd64 GLib snapd library
ii libsndfile1 1.0.25-10ubuntu0.16.04.1 amd64 Library for reading/writing audio files
ii libsnmp-base 5.7.3+dfsg-1ubuntu4.2 all SNMP configuration script, MIBs and documentation
ii libsnmp30 5.7.3+dfsg-1ubuntu4.2 amd64 SNMP (Simple Network Management Protocol) library
ii libsocket6-perl 0.25-1build2 amd64 Perl extensions for IPv6
ii libodium23 1.0.18-1+ubuntu16.04.1+deb.sury.org+1 amd64 Network communication, cryptography and signaturing library
ii libsonice0 0.2.0-3 amd64 Simple library to speed up or slow down speech
ii libsoup-gnome2.4-1 2.52.2-1ubuntu0.3 amd64 HTTP library implementation in C -- GNOME support library
ii libsox2p2.4-1 2.52.2-1ubuntu0.3 amd64 HTTP library implementation in C -- Shared library
ii libspectre1 0.2.7-3ubuntu2 amd64 Library for rendering PostScript documents
ii libspeexd2 0.8.3-1ubuntu3 amd64 Speech Dispatcher: Shared libraries
ii libspeex1 1.2~rc1.2-1ubuntu1 amd64 The Speex codec runtime library
ii libspeexdsp1 1.2~rc1.2-1ubuntu1 amd64 The Speex extended runtime library
ii libsqlite3-0 3.11.0-1ubuntu1.1 amd64 SQLite 3 shared library
ii libss2 1.42.13-1ubuntu1 amd64 command-line interface parsing library
ii libssh-4 0.6.3-4.3ubuntu0.2 amd64 tiny C SSH library (OpenSSL flavor)
ii libss11.0-0 1.0.2g-1ubuntu4.14 amd64 Secure Sockets Layer toolkit - shared libraries
ii libss11.1 1.1.1-1.1.1g-1+ubuntu16.04.1+deb.sury.org+1 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstartup-notification0 0.12.4~build1 amd64 library for program launch feedback (shared library)
ii libstdc++-5-dev 5.4.0-6ubuntu1~16.04.11 amd64 GNU Standard C++ Library v3 (development files)
ii libsub-name-perl 0.14-1build1 amd64 module for assigning a new name to referenced sub
ii libsuitesparseconfig4.4.6 1:4.4.6-1 amd64 configuration routines for all SuiteSparse modules
ii libsystemd0 229-4ubuntu21.16 amd64 systemd utility library
ii libtag1v5 1.9.1-2.4ubuntu1 amd64 audio meta-data library
ii libtag1v5-vanilla 1.9.1-2.4ubuntu1 amd64 audio meta-data library - vanilla flavour
ii libtalloc2 2.1.5-2 amd64 hierarchical pool based memory allocator
ii libtasn1-6 4.7-3ubuntu0.16.04.3 amd64 Manage ASN.1 structures (runtime)
ii libtcl8.6 8.6.5+dfsg-2 amd64 Tcl (the Tool Command Language) v8.6 - run-time library files
ii libtdb1 3.1.8-2 amd64 Trivial Database - shared library
ii libtelepathy-glib0 0.24.1-1.1 amd64 Telepathy framework - GLib library
ii libterm-readkey-perl 2.33-1build1 amd64 perl module for simple terminal control
ii libtevent0 0.9.28-0ubuntu0.16.04.1 amd64 malloc-based event loop library - shared library
ii libtext-charwidth-perl 0.04-7build5 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5build4 amd64 converts between character sets in Perl
ii libtext-levenshtein-perl 0.13-1 all implementation of the Levenshtein edit distance
ii libtext-wrapi8n-perl 0.06-7.1 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.24-2 all Data files for Thai language support library
ii libthraora0 0.1.1+dfsg.1-8 amd64 Theora Video Compression Codec
ii libtie-ixhash-perl 1.23-2 all Perl module to order associative arrays
ii libtiff5 4.0.6-1ubuntu0.5 amd64 Tag Image File Format (TIFF) library
ii libtimedate-perl 2.3000-2 all collection of modules to manipulate date/time information
ii libtimezonemap-data 0.4.5 all GTK+3 timezone map widget - data files
ii libtimezonemap1 0.4.5 amd64 GTK+3 timezone map widget
ii libtinfo5 6.0+20160213-1ubuntu1 amd64 shared low-level terminfo library for terminal handling
ii libtk8.6 8.6.5-1 amd64 Tk toolkit for Tcl and X11 v8.6 - run-time files
ii libtotem-plparser-common 3.10.6-1ubuntu1 all Totem Playlist Parser library - common files
ii libtotem-plparser18 3.10.6-1ubuntu1 amd64 Totem Playlist Parser library - runtime files
ii libtotem0 3.18.1-1ubuntu4 amd64 Main library for the Totem media player
ii libtracker-spargl-1.0-0 1.6.2-0ubuntu1.1 amd64 metadata database, indexer and search tool - library
ii libtsan0 5.4.0-6ubuntu1~16.04.11 amd64 ThreadSanitizer -- a Valgrind-based detector of data races (runtime)
ii libtxc-dxtn-s2tc0 0~git20131104-1.1 amd64 Texture compression library for Mesa
ii libubsan0 5.4.0-6ubuntu1~16.04.11 amd64 UBSan -- undefined behaviour sanitizer (runtime)
ii libubuntustegestures5 1.3.1918+16.04.20160404-0ubuntu1 amd64 Ubuntu gestures library for Ubuntu UI Toolkit
ii libubuntutoolkit5 1.3.1918+16.04.20160404-0ubuntu1 amd64 Ubuntu toolkit common library for Ubuntu UI Toolkit
ii libudev1 229-4ubuntu21.16 amd64 libudev shared library
ii libudisks2-0 2.1.7-1ubuntu1 amd64 GObject based library to access udisks2
ii libunistring0 0.9.3-5.2ubuntu1 amd64 Unicode string library for C
ii libunity-action-qt1 1.1.0+14.04.20140304-0ubuntu2~gcc5.1 amd64 Unity Action Qt API
ii libunity-control-center1 15.04.0+16.04.20171130-0ubuntu1 amd64 utilities to configure the GNOME desktop
ii libunity-core-6.0-9 7.4.5+16.04.20180221-0ubuntu1 amd64 core library for the Unity interface
ii libunity-gtk2-parser0 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell to GMenuModel parser
ii libunity-gtk3-parser0 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell to GMenuModel parser
ii libunity-misc4 4.0.5+14.04.20140115-0ubuntu1 amd64 Miscellaneous functions for Unity - shared library
ii libunity-protocol-private0 7.1.1+16.04.20180209.1-0ubuntu1 amd64 binding to get places into the launcher - private library
ii libunity-scopes-json-def-desktop7 7.1.1+16.04.20180209.1-0ubuntu1 all binding to get places into the launcher - desktop def file
ii libunity-settings-daemon1 15.04.1+16.04.20160701-0ubuntu3 amd64 Helper library for accessing settings
ii libunity-webapps0 2.5.0+16.04.20160201-0ubuntu1 amd64 Web Apps integration with the Unity desktop
ii libunibody9 7.1.1+16.04.20180209.1-0ubuntu1 amd64 binding to get places into the launcher - shared library
ii libunwind8 1.1-4.1 amd64 library to determine the call-chain of a program - runtime
ii libupower-glib3 0.99.4-2ubuntu0.3 amd64 abstraction for power management - shared library
ii liburi-perl 1.71-1 all module to manipulate and access URI strings
ii liburl-dispatcher1 0.1+16.04.20151110-0ubuntu2 amd64 library for sending requests to the url dispatcher
ii libusb-0.1-4 2:0.1.12-28 amd64 userspace USB programming library
ii libusb-1.0-0 2:1.0.20-1 amd64 userspace USB programming library
ii libusbxmud4 1.0.10-2ubuntu0.1 amd64 USB multiplexor daemon for iPhone and iPod Touch devices - library
ii libustr-1.0-1 1.0.4-5 amd64 Micro string library: shared library
ii libutempter0 1.1.6-3 amd64 privileged helper for utmp/wtmp updates (runtime)
ii libuuid-perl 0.24-1build1 amd64 Perl extension for using UUID interfaces as defined in e2fsprogs
ii libuuuid1 2.27.1-6ubuntu3.6 amd64 Universally Unique ID library
ii libv4lconvert0 1.10.0-1 amd64 Video4linux frame format conversion library
ii libvisio-0.1-1 0.1.5-1ubuntu1 amd64 library for parsing the visio file structure
ii libvisual-0.4-0 0.4.0-8 amd64 audio visualization framework
ii libvncclient1 0.9.10+dfsg-3ubuntu0.16.04.3 amd64 API to write one's own VNC server - client library
ii libvorbis0a 1.3.5-3ubuntu0.2 amd64 decoder library for Vorbis General Audio Compression Codec
ii libvorbisenc2 1.3.5-3ubuntu0.2 amd64 encoder library for Vorbis General Audio Compression Codec

```

```

ii libvorbisfile3.1.3.5-3ubuntu0.2 amd64 high-level API for Vorbis General Audio Compression Codec
ii libvpx3 1.5.0-2ubuntu1 amd64 VP8 and VP9 video codec (shared library)
ii libvte-2.91-0 0.42.5-1ubuntu1 amd64 Terminal emulator widget for GTK+ 3.0 - runtime files
ii libvte-2.91-common 0.42.5-1ubuntu1 all Terminal emulator widget for GTK+ 3.0 - common files
ii libwacom-bin 0.22-1~ubuntu16.04.1 amd64 Wacom model feature query library -- binaries
ii libwacom-common 0.22-1~ubuntu16.04.1 all Wacom model feature query library (common files)
ii libwacom2 0.22-1~ubuntu16.04.1 amd64 Wacom model feature query library
ii libwavpack1 4.75.2-2ubuntu0.2 amd64 audio codec (lossy and lossless) - library
ii libwayland-client0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - client library
ii libwayland-cursor0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - cursor library
ii libwayland-egl1-mesa 18.0.5-0ubuntu0~16.04.1 amd64 implementation of the Wayland EGL platform -- runtime
ii libwayland-server0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - server library
ii libwebkitclient0 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Samba winbind client library
ii libwebkit2gtk-4.0-37 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+
ii libwebkit2gtk-4.0-37-gtk2 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+ - GTK2 plugin process
ii libwebp5 0.4.4-1 amd64 Lossy compression of digital photographic images.
ii libwebpdemux1 0.4.4-1 amd64 Lossy compression of digital photographic images.
ii libwebpmux1 0.4.4-1 amd64 Lossy compression of digital photographic images.
ii libwebrtc-audio-processing-0 0.1-3ubuntu1~gcc5.1 amd64 AudioProcessing module from the WebRTC project.
ii libwhoopsie-preferences0 0.18 amd64 Ubuntu error tracker submission settings - shared library
ii libwhoopsie0 0.2.52.5 amd64 Ubuntu error tracker submission - shared library
ii libwindo-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - stringprep implementation
ii libwinpr-crt0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (crt library)
ii libwinpr-dsparse0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (dsparse library)
ii libwinpr-environment0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (environment library)
ii libwinpr-file0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (file library)
ii libwinpr-handle0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (handle library)
ii libwinpr-heap0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (heap library)
ii libwinpr-input0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (input library)
ii libwinpr-interlocked0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (interlocked library)
ii libwinpr-library0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (library)
ii libwinpr-path0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (path library)
ii libwinpr-pool0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (pool library)
ii libwinpr-registry0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (registry library)
ii libwinpr-rpc0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (RPC library)
ii libwinpr-sspi0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (sspi library)
ii libwinpr-synch0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (synch library)
ii libwinpr-sysinfo0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (sysinfo library)
ii libwinpr-thread0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (thread library)
ii libwinpr-utils0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.3 amd64 Windows Portable Runtime library (utils library)
ii libwmf0.2-7 0.2.8.4-10.5ubuntu1 amd64 Windows metafile conversion library
ii libwmf0.2-7-gtk 0.2.8.4-10.5ubuntu1 amd64 Windows metafile conversion library
ii libwnck-3-0 3.14.1-2 amd64 Window Navigator Construction Kit - runtime files
ii libwnck-3-common 3.14.1-2 all Window Navigator Construction Kit - common files
ii libwpd-0.10-10 0.10.1~ubuntu1 amd64 Library for handling WordPerfect documents (shared library)
ii libwpdg-0.3-3 0.3.1~ubuntu1 amd64 WordPerfect graphics import/convert library (shared library)
ii libwps-0.4-4 0.4.3-1ubuntu1 amd64 Works text file format import filter library (shared library)
ii libwrap0 7.6.q-25 amd64 Wietse Venema's TCP wrappers library
ii libwww-perl 6.15-1 all simple and consistent interface to the world-wide web
ii libwww-robotrules-perl 6.01-1 all database of robots.txt-derived permissions
ii libx11-6 2:1.6.3-1ubuntu2.1 amd64 X11 client-side library
ii libx11-data 2:1.6.3-1ubuntu2.1 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 2:1.6.3-1ubuntu2.1 amd64 Xlib/XCB interface library
ii libx86-1 1.1+ds1-10 amd64 x86 real-mode library
ii libxapian22v5 1.2.22-2 amd64 Search engine library
ii libxatracker2 18.0.5-0ubuntu0~16.04.1 amd64 X acceleration library -- runtime
ii libxaugd 1:1.0.8-1 amd64 X11 authorisation library
ii libxaw7 2:1.0.13-1 amd64 X11 Athena Widget library
ii libxcb-dri2-0 1.11.1-1ubuntu1 amd64 X C Binding, dri2 extension
ii libxcb-data 1.11.1-1ubuntu1 amd64 X C Binding, dri2 extension
ii libxcb-dri3-0 1.11.1-1ubuntu1 amd64 X C Binding, dri3 extension
ii libxcb-glx0 1.11.1-1ubuntu1 amd64 X C Binding, glx extension
ii libxcb-icccm4 0.4.1-1ubuntu1 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 0.4.0-1 amd64 utility libraries for X C Binding -- keysyms
ii libxcb-present0 1.11.1-1ubuntu1 amd64 X C Binding, present extension
ii libxcb-randr0 1.11.1-1ubuntu1 amd64 X C Binding, randr extension
ii libxcb-render-util0 0.3.9-1 amd64 utility libraries for X C Binding -- render-util
ii libxcb-render0 1.11.1-1ubuntu1 amd64 X C Binding, render extension
ii libxcb-shape0 1.11.1-1ubuntu1 amd64 X C Binding, shape extension
ii libxcb-shm0 1.11.1-1ubuntu1 amd64 X C Binding, shm extension
ii libxcb-sync1 1.11.1-1ubuntu1 amd64 X C Binding, sync extension
ii libxcb-util0 0.4.0-0ubuntu3 amd64 utility libraries for X C Binding -- atom, aux and event
ii libxcb-xfixes0 1.11.1-1ubuntu1 amd64 X C Binding, xfixes extension
ii libxcb-xkb1 1.11.1-1ubuntu1 amd64 X C Binding, XKEYBOARD extension
ii libxcb-xkb1 1.11.1-1ubuntu1 amd64 X C Binding
ii libcomposite1 1:0.4.4-1 amd64 X11 Composite extension library
ii libcursor1 1:1.1.14-1ubuntu0.16.04.2 amd64 X cursor management library
ii libxdamage1 1:1.1.4-2 amd64 X11 damaged region extension library
ii libxdmcp6 1:1.1.2-1.1 amd64 X11 Display Mañager Control Protocol library
ii libxext6 2:1.3.3-1 amd64 X11 miscellaneous extension library
ii libxfixes3 1:5.0.1-2 amd64 X11 miscellaneous 'fixes' extension library
ii libxfont1 1:1.5.1-1ubuntu0.16.04.4 amd64 X11 font rasterisation library
ii libxfont2 1:2.0.1-3ubuntu16.04.3 amd64 X11 font rasterisation library
ii libxft2 2.3.2-1 amd64 FreeType-based font drawing library for X
ii libxi6 2:1.7.6-1 amd64 X11 Input extension library
ii libxinerama1 2:1.1.3-1 amd64 X11 Xinerama extension library
ii libxkbcommon-x11-0 0.5.0-1ubuntu2.1 amd64 library to create keymaps with the XKB X11 protocol
ii libxkbcommon0 0.5.0-1ubuntu2.1 amd64 library interface to the XKB compiler - shared library
ii libxkbfile1 1:1.0.9-0ubuntu1 amd64 X11 keyboard file manipulation library
ii libxklavier16 5.4-0ubuntu2 amd64 X Keyboard Extension high-level API
ii libxml-parser-perl 2.44-1build1 amd64 Perl module for parsing XML files
ii libxml-twig-perl 1:3.48-1 all Perl module for processing huge XML documents in tree mode
ii libxml-xpathengine-perl 0.13-1 all re-usable XPath engine for DOM-like trees
ii libxml1 2.9.3+dfsg1-1ubuntu0.6 amd64 GNOME XML library
ii libxmlrpc-epi0 0.54.2-1ubuntu0.1 amd64 XML-RPC request serialisation/deserialisation library
ii libxmug6 2:1.1.2-2 amd64 X11 miscellaneous utility library
ii libxmui1 2:1.1.2-2 amd64 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.11-1ubuntu0.16.04.1 amd64 X11 pixmap library

```

```

ii libxrandr2 2:1.5.0-1 amd64 X11 RandR extension library
ii libxrender1 1:0.9.9-0ubuntu1 amd64 X Rendering Extension client library
ii libxres1 2:1.0.7-1 amd64 X11 Resource extension library
ii libxshmfence1 1.2.1 amd64 X shared memory fences - shared library
ii libxslt1 1:1.1.28-2.1ubuntu0.1 amd64 XSLT 1.0 processing library - runtime library
ii libxss1 1:1.2.2-1 amd64 X11 Screen Saver extension library
ii libxt6 1:1.1.5-0ubuntu1 amd64 X11 toolkit intrinsics library
ii libxtables1 1:6.0-2ubuntu3 amd64 netfilter xtables library
ii libxtst6 2:1.2.2-1 amd64 X11 Testing -- Record extension library
ii libxv1 2:1.0.10-1 amd64 X11 Video extension library
ii libxvmc1 2:1.0.9-1ubuntu1 amd64 X11 Video extension library
ii libxxf86dg1 2:1.1.4-1 amd64 X11 Direct Graphics Access extension library
ii libxxf86vm1 1:1.1.4-1 amd64 X11 XFree86 video mode extension library
ii libyaml1 2.1.0-2 amd64 Yet Another JSON Library
ii libyaml-0-2 0.1.6-3 amd64 Fast YAML 1.1 parser and emitter library
ii libyaml-perl 0.41-6build1 amd64 Perl interface to libyaml, a YAML implementation
ii libyaml-tiny-perl 1.69-1 all Perl module for reading and writing YAML files
ii libyelp0 3.18.1-1ubuntu4 amd64 Library for the GNOME help browser
ii libzeitgeist-1.0-0 0.3.18-1ubuntu3 amd64 library to access Zeitgeist - shared library
ii libzeitgeist-2.0-0 0.3.16-0ubuntu4 amd64 library to access Zeitgeist - shared library
ii libzip4 1.6.1-3+ubuntu16.04.1+deb.sury.org+2 amd64 library for reading, creating, and modifying zip archives (runtime)
ii light-themes 14.04+16.04.20180326-0ubuntu1 all Light Themes (Ambiance and Radiance)
ii lightdm 1.18.3-0ubuntu1.1 amd64 Display Manager
ii lintian 2.5.43ubuntu0.1 all Debian package checker
ii linux-base 4.5ubuntu1~16.04.1 all Linux image base package
ii linux-firmware 1.157.21 all Firmware for Linux kernel drivers
ii linux-generic-hwe-16.04 4.15.0.45.66 amd64 Complete Generic Linux kernel and headers
ii linux-headers-4.15.0-45 4.15.0-45.48-16.04.1 all Header files related to Linux kernel version 4.15.0
ii linux-headers-4.15.0-45-generic 4.15.0-45.48-16.04.1 amd64 Linux kernel headers for version 4.15.0 on 64 bit x86 SMP
ii linux-headers-generic-hwe-16.04 4.15.0-45.66 amd64 Generic Linux kernel headers
ii linux-image-4.15.0-45-generic 4.15.0-45.48-16.04.1 amd64 Signed kernel image generic
ii linux-image-generic-hwe-16.04 4.15.0-45.66 amd64 Generic Linux kernel image
ii linux-libc-dev 4.4.0-142.168 amd64 Linux Kernel Headers for development
ii linux-modules-4.15.0-45-generic 4.15.0-45.48-16.04.1 amd64 Linux kernel extra modules for version 4.15.0 on 64 bit x86 SMP
ii linux-modules-extra-4.15.0-45-generic 4.15.0-45.48-16.04.1 amd64 Linux kernel extra modules for version 4.15.0 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 2.23-0ubuntu11 all GNU C Library: National Language (locale) data [support]
ii login 1:4.2-3.1ubuntu5.3 amd64 system login tools
ii logrotate 3.8.7-2ubuntu2.16.04.2 amd64 Log rotation utility
ii lp-solve 5.5.0.13-7build2 amd64 Solve (mixed integer) linear programming problems
ii lsb-base 9.20160110ubuntu0.2 all Linux Standard Base init script functionality
ii lsb-release 9.20160110ubuntu0.2 all Linux Standard Base version reporting utility
ii lshw 02.17-1.1ubuntu3.5 amd64 information about hardware configuration
ii lsof 4.89+dfsg-0.1 amd64 Utility to list open files
ii ltrace 0.7.3-5.1ubuntu4 amd64 Tracks runtime library calls in dynamically linked programs
ii make 4.1-6 amd64 utility for directing compilation
ii makedev 2.3.1-93ubuntu2~ubuntu16.04.1 all creates device files in /dev
ii man-db 2.7.5-1 amd64 on-line manual pager
ii manpages 4.04-2 all Manual pages about using a GNU/Linux system
ii manpages-dev 4.04-2 all Manual pages about using GNU/Linux for development
ii mariadb-client 10.0.38-0ubuntu0.16.04.1 all MariaDB database client (metapackage depending on the latest version)
ii mariadb-client-10.0 10.0.38-0ubuntu0.16.04.1 amd64 MariaDB database client binaries
ii mariadb-client-core-10.0 10.0.38-0ubuntu0.16.04.1 amd64 MariaDB database core client binaries
ii mariadb-common 10.0.38-0ubuntu0.16.04.1 all MariaDB common metapackage
ii mariadb-server 10.0.38-0ubuntu0.16.04.1 all MariaDB database server (metapackage depending on the latest version)
ii mariadb-server-10.0 10.0.38-0ubuntu0.16.04.1 amd64 MariaDB database server binaries
ii mariadb-server-core-10.0 10.0.38-0ubuntu0.16.04.1 amd64 MariaDB database core server files
ii mawk 1.3.3-17ubuntu2 amd64 a pattern scanning and text processing language
ii media-player-info 22-2 all Media player identification files
ii memtest86+ 5.01-3ubuntu2 amd64 thorough real-mode memory tester
ii metacity-common 1:3.18.7-0ubuntu0.3 all shared files for the Metacity window manager
ii mime-support 3.59ubuntu1 all MIME files 'mime.types' & 'mailcap', and support programs
ii mlocate 0.26-1ubuntu2 amd64 quickly find files on the filesystem based on their name
ii mobile-broadband-provider-info 20140317-1 all database of mobile broadband service providers
ii modemmanager 1.6.4-1ubuntu0.16.04.1 amd64 D-Bus service for managing modems
ii mount 2.27.1-6ubuntu3.6 amd64 tools for mounting and manipulating filesystems
ii mountall 2.54ubuntu1 amd64 filesystem mounting tool
ii mousetweaks 3.12.0-1ubuntu2 amd64 mouse accessibility enhancements for the GNOME desktop
ii mscompress 0.4-3 amd64 Microsoft "compress.exe/expand.exe" compatible (de)compressor
ii mtools 4.0.18-2ubuntu0.16.04 amd64 Tools for manipulating MSDOS files
ii mtr-tiny 0.86-1ubuntu0.1 amd64 Full screen ncurses traceroute tool
ii multiarch-support 2.23-0ubuntu11 amd64 Transitional package to ensure multiarch compatibility
ii mysql-common 5.7.30-0ubuntu0.16.04.1 all MySQL database common files, e.g. /etc/mysql/my.cnf
ii mythes-en-us 1:5.1.0-1ubuntu2.2 all English (USA) Thesaurus for LibreOffice
ii nano 2.5.3-2ubuntu2 amd64 small, friendly text editor inspired by Pico
ii nautilus 1:3.18.4.1s.3.14.3-0ubuntu6 amd64 file manager and graphical shell for GNOME
ii nautilus-data 1:3.18.4.1s.3.14.3-0ubuntu6 all data files for nautilus
ii nautilus-sendto 3.8.2-1ubuntu1 amd64 integrates Evolution and Pidgin into the Nautilus file manager
ii nautilus-share 0.7.3-2ubuntu1 amd64 Nautilus extension to share folder using Samba
ii ncurses-base 6.0+20160213-1ubuntu1 all basic terminal type definitions
ii ncurses-bin 6.0+20160213-1ubuntu1 amd64 terminal-related programs and man pages
ii ncurses-term 6.0+20160213-1ubuntu1 all additional terminal type definitions
ii net-tools 1.60-26ubuntu1 amd64 NET-3 networking toolkit
ii netbase 5.3 all Basic TCP/IP networking system
ii netcat-openbsd 1.105-7ubuntu1 amd64 TCP/IP swiss army knife
ii netpbm 2:10.0-15.3 amd64 Graphics conversion tools between image formats
ii network-manager 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (daemon_and_userspace_tools)
ii network-manager-gnome 1.2.6-0ubuntu0.16.04.4 amd64 network management framework (GNOME frontend)
ii network-manager-pptp 1.1.93-1ubuntu1 amd64 network management framework (PPTP plugin core)
ii network-manager-pptp-gnome 1.1.93-1ubuntu1 amd64 network management framework (PPTP plugin GNOME GUI)
ii notify OSD 0.9.35+16.04.20160415-0ubuntu1 amd64 daemon that displays passive pop-up notifications
ii notify OSD icons 0.8+15.10.20151016.2-0ubuntu1 all Notify-OSD icons
ii ntfs-3g 1:2015.3-144R.1-1ubuntu0.1 amd64 read/write NTFS driver for FUSE
ii nux-tools 4.0.8+16.04.20180622.2-0ubuntu1 amd64 Visual rendering toolkit for real-time applications - tools
ii onboard 1.2.0-0ubuntu5 amd64 Simple On-screen Keyboard
ii onboard-data 1.2.0-0ubuntu5 all Language model files for the word suggestion feature of Onboard
ii openoffice.org-hyphenation 0.9 all Hyphenation patterns for OpenOffice.org
ii openprinting-ppds 20160212-0ubuntu1 all OpenPrinting printer support - PostScript PPD files
ii openssh-client 1:7.2p2-4ubuntu2.10 amd64 secure shell (SSH) client, for secure access to remote machines

```

```

ii openssh-server 1:7.2p2-4ubuntu2.10 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:7.2p2-4ubuntu2.10 amd64 secure shell (SSH) sFTP server module, for SFTP access from remote machines
ii openssl 1.0.2g-1ubuntu0.14 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii os-prober 1.7.0ubuntu3.3 amd64 utility to detect other OSes on a set of drives
ii overlay-scrollbar 0.2.17.1+16.04.20151117-0ubuntu1.16.04.1 all Scrollbar overlay - configuration
ii overlay-scrollbar-gtk2 0.2.17.1+16.04.20151117-0ubuntu1.16.04.1 amd64 GTK 2 module for overlay scrollbars
ii oxideqt-codecs 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (codecs)
ii p11-kit 0.23.2-5~ubuntu16.04.1 amd64 p11-glue utilities
ii p11-kit-modules 0.23.2-5~ubuntu16.04.1 amd64 p11-glue proxy and trust modules
ii parted 3.2-15ubuntu0.1 amd64 disk partition manipulator
ii passwd 1:4.2-3.1ubuntu5.3 amd64 change and administer password and group data
ii patch 2.7.5-1ubuntu0.16.04.1 amd64 Apply a diff file to an original
ii patchutils 0.3.4-1 amd64 Utilities to work with patches
ii pciutils 1:3.3.1-1.1ubuntu1.3 amd64 Linux PCI Utilities
ii pcmciautils 018-8 amd64 PCMCIA utilities for Linux 2.6
ii perl 5.22.1-9ubuntu0.6 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.22.1-9ubuntu0.6 amd64 minimal Perl system
ii perl-modules-5.22 5.22.1-9ubuntu0.6 all Core Perl modules
ii php-common 2:76+ubuntu16.04.1+deb.sury.org+9 all Common files for PHP packages
ii php7.2 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 all server-side, HTML-embedded scripting language (metapackage)
ii php7.2-cli 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 command-line interpreter for the PHP scripting language
ii php7.2-common 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 documentation, examples and common module for PHP
ii php7.2-curl 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 CURL module for PHP
ii php7.2-gd 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 GD module for PHP
ii php7.2-intl 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 Internationalisation module for PHP
ii php7.2-json 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 JSON module for PHP
ii php7.2-mbstring 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 MBSTRING module for PHP
ii php7.2-mysql 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 MySQL module for PHP
ii php7.2-opcache 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 Zend OpCache module for PHP
ii php7.2-readline 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 readline module for PHP
ii php7.2-sqlite3 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 SQLite3 module for PHP
ii php7.2-xml 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 DOM, SimpleXML, WDDX, XML, and XSL module for PHP
ii php7.2-xmlrpc 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 XMLRPC-EPI module for PHP
ii php7.2-zip 7.2.32-1+ubuntu16.04.1+deb.sury.org+1 amd64 Zip module for PHP
ii pinentry-curses 0.9.7-3 amd64 curses-based PIN or pass-phrase entry dialog for GnuPG
ii pinentry-gnome3 0.9.7-3 amd64 GNOME 3 PIN or pass-phrase entry dialog for GnuPG
ii pkg-config 0.29.1-0ubuntu1 amd64 manage compile and link flags for libraries
ii plainbox-provider-checkbox 0.25-1 amd64 CheckBox provider for PlainBox
ii plainbox-provider-resource-generic 0.23-1 amd64 CheckBox generic resource jobs provider
ii plainbox-secure-policy 0.25-1 all policykit policy required to use plainbox (secure version)
ii plymouth 0.9.2-3ubuntu13.5 amd64 boot animation, logger and I/O multiplexer
ii plymouth-label 0.9.2-3ubuntu13.5 amd64 boot animation, logger and I/O multiplexer - label control
ii plymouth-theme-ubuntu-logo 0.9.2-3ubuntu13.5 amd64 boot animation, logger and I/O multiplexer - ubuntu theme
ii plymouth-theme-ubuntu-text 0.9.2-3ubuntu13.5 amd64 boot animation, logger and I/O multiplexer - ubuntu text theme
ii pm-utils 1.4.1-16 all utilities and scripts for power management
ii policykit-1 0.105-14.1ubuntu0.4 amd64 framework for managing administrative policies and privileges
ii policykit-1-gnome 0.105-2ubuntu2 amd64 GNOME authentication agent for PolicyKit-1
ii policykit-desktop-privileges 0.20 all run common desktop actions without password
ii poppler-data 0.4.7-7 all Encoding data for the poppler PDF rendering library
ii poppler-utils 0.41.0-0ubuntu1.12 amd64 PDF utilities (based on Poppler)
ii popularity-contest 1.64ubuntu2 all Vote for your favourite packages automatically
ii powermgmt-base 1.31+nmu1.all Common utils and configs for power management
ii ppp 2.4.7-14ubuntu1.16.04.1 amd64 Point-to-Point Protocol (PPP) - daemon
ii pppconfig 2.3.22 all Text menu based utility for configuring ppp
ii pppoeconf 1.21ubuntu1.all configures PPPoE/ADSL connections
ii pptp-linux 1.8.0-1 amd64 Point-to-Point Tunneling Protocol (PPTP) Client
ii printer-driver-brlaser 3-5ubuntu1 amd64 printer driver for (some) Brother laser printers
ii printer-driver-c2esp 27-2 amd64 printer driver for Kodak ESP AiO color inkjet Series
ii printer-driver-foo2zjs 20151024dfsg0-1ubuntu1 amd64 printer driver for ZjStream-based printers
ii printer-driver-foo2zjs-common 20151024dfsg0-1ubuntu1 all printer driver for ZjStream-based printers - common files
ii printer-driver-gutenprint 5.2.11-1 amd64 printer drivers for CUPS
ii printer-driver-hpcups 3.16.3+repack0-1 amd64 HP Linux Printing and Imaging - CUPS Raster driver (hpcups)
ii printer-driver-min12xxw 0.0.9-9 amd64 printer driver for KonicaMinolta PagePro 1[234]xxW
ii printer-driver-pnm2ppa 1.13+nondbs-0ubuntu5 amd64 printer driver for HP-GDI printers
ii printer-driver-postscript-hp 3.16.3+repack0-1 all HP Printers PostScript Descriptions
ii printer-driver-ptouch 1.4-1 amd64 printer driver Brother P-touch label printers
ii printer-driver-pxljr 1.4+repack0-4 amd64 printer driver for HP Color LaserJet 35xx/36xx
ii printer-driver-sag-gdi 0.1-4ubuntu1 all printer driver for Ricoh Aficio SP 1000s/SP 1100s
ii printer-driver-splix 2.0.0+svn315-4fakesync1 amd64 Driver for Samsung and Xerox SPL2 and SPLc laser printers
ii procps 2:3.3.10-4ubuntu2.4 amd64 /proc file system utilities
ii psmisc 22.21-2.1build1 amd64 utilities that use the proc file system
ii pulseaudio 1:8.0-0ubuntu3.10 amd64 PulseAudio sound server
ii pulseaudio-module-bluetooth 1:8.0-0ubuntu3.10 amd64 Bluetooth module for PulseAudio sound server
ii pulseaudio-module-x11 1:8.0-0ubuntu3.10 amd64 X11 module for PulseAudio sound server
ii pulseaudio-utils 1:8.0-0ubuntu3.10 amd64 Command line tools for the PulseAudio sound server
ii pyotherside 1.4.0-2 all transitional dummy package
ii python 2.7.12-1-16.04 amd64 interactive high-level object-oriented language (default version)
ii python-apt-common 1.1.0~beta1ubuntu0.16.04.2 all Python interface to libapt-pkg (locales)
ii python-crypto 2.6.1-6ubuntu0.16.04.3 amd64 cryptographic algorithms and protocols for Python
ii python-dnspython 1.12.0-1 all DNS toolkit for Python
ii python-ldb 2:1.1.24-1ubuntu3.1 amd64 Python bindings for LDB
ii python-minimal 2.7.12-1~16.04 amd64 minimal subset of the Python language (default version)
ii python-samba 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Python bindings for Samba
ii python-talloc 2.1.5-2 amd64 hierarchical pool based memory allocator - Python bindings
ii python-tdb 1.3.8-2 amd64 Python bindings for TDB
ii python2.7 2.7.12-1ubuntu0-16.04.4 amd64 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.12-1ubuntu0-16.04.4 amd64 Minimal subset of the Python language (version 2.7)
ii python3 3.5.1-3 amd64 interactive high-level object-oriented language (default python3 version)
ii python3-apport 2.20.1-0ubuntu2.18 all Python 3 library for Apport crash report handling
ii python3-apt 1.1.0~beta1ubuntu0.16.04.2 amd64 Python 3 interface to libapt-pkg
ii python3-aptdaemon 1.1.1+bzr982-0ubuntu14 all Python 3 module for the server and client of aptdaemon
ii python3-aptdaemon.gtk3widgets 1.1.1+bzr982-0ubuntu14 all Python 3 GTK+ 3 widgets to run an aptdaemon client
ii python3-aptdaemon.pkcompat 1.1.1+bzr982-0ubuntu14 all PackageKit compatibility for AptDaemon
ii python3-blinker 1.3.0+dfsg-1ubuntu1 all fast, simple object-to-object and broadcast signaling library
ii python3-brlapi 5.3.1-2ubuntu2.1 amd64 Braille display access via BRLTTY - Python3 bindings
ii python3-bs4 4.4.1-1 all error-tolerant HTML parser for Python 3
ii python3-cairo 1.10.0+dfsg-5ubuntu1 amd64 Python 3 bindings for the Cairo vector graphics library
ii python3-cffi-backend 1.5.2-1ubuntu1 amd64 Foreign Function Interface for Python 3 calling C code - runtime
ii python3-chardet 2.3.0-2 all universal character encoding detector for Python3

```

```

ii python3-checkbox-support 0.22-1 all collection of Python modules used by PlainBox providers
ii python3-commandnotfound 0.3ubuntu16.04.2 all Python 3 bindings for command-not-found.
ii python3-cryptography 1.2.3-1ubuntu0.2 amd64 Python library exposing cryptographic recipes and primitives (Python 3)
ii python3-cups 1.9.73-0ubuntu2 amd64 Python3 bindings for CUPS
ii python3-cupshelpers 1.5.7+20160212-0ubuntu2 all Python modules for printer configuration with CUPS
ii python3-dbus 1.2.0-3 amd64 simple interprocess messaging system (Python 3 interface)
ii python3-debian 0.1.27ubuntu2 all Python 3 modules to work with Debian-related data formats
ii python3-defer 1.0.6-2build1 all Small framework for asynchronous programming (Python 3)
ii python3-distupgrade 1:16.04.26 all manage release upgrades
ii python3-feedparser 5.1.3-3build1 all Universal Feed Parser for Python 3
ii python3-gdbm 3.5.1-1 amd64 GNU dbm database support for Python 3-x
ii python3-gi 3.20.0-0ubuntu1 amd64 Python 3 bindings for gobject-introspection libraries
ii python3-gi-cairo 3.20.0-0ubuntu1 amd64 Python 3 Cairo bindings for the GObject library
ii python3-quacamole 0.9.2-1 all framework for creating command line applications (Python 3)
ii python3-htmllib 0.999-4 all HTML parser/tokenizer based on the WHATWG HTML5 specification (Python 3)
ii python3-httplib2 0.9.1+dfsg-1 all comprehensive HTTP client library written for Python3
ii python3-idna 2.0-3 all Python IDNA2008 (RFC 5891) handling (Python 3)
ii python3-jinja2 2.8-1 all small but fast and easy to use stand-alone template engine
ii python3-jwt 1.3.0-1ubuntu0.1 all Python 3 implementation of JSON Web Token
ii python3-louis 2.6.4-2ubuntu0.4 all Python bindings for liblouis
ii python3-lxml 3.5.0-1ubuntu0.1 amd64 pythonic binding for the libxml2 and libxslt libraries
ii python3-mako 1.0.3+ds1-1ubuntu1 all fast and lightweight templating for the Python 3 platform
ii python3-markupsafe 0.23-2build2 amd64 HTML/XHTML/XML string library for Python 3
ii python3-minimal 3.5.1-3 amd64 minimal subset of the Python language (default python3 version)
ii python3-oauthlib 1.0.3-1 all generic, spec-compliant implementation of OAuth for Python3
ii python3-padme 1.1.1-2 all mostly transparent proxy class for Python 3
ii python3-pexpect 4.0.1-1 all Python 3 module for automating interactive applications
ii python3-pil 3.1.2-0ubuntu1.1 amd64 Python Imaging Library (Python3)
ii python3-pkg-resources 20.7.0-1 all Package Discovery and Resource Access using pkg_resources
ii python3-plainbox 0.25-1 all toolkit for software and hardware testing (python3 module)
ii python3-problem-report 2.20.1-0ubuntu2.18 all Python 3 library to handle problem reports
ii python3-ptyprocess 0.5-1 all Run a subprocess in a pseudo terminal from Python 3
ii python3-pysn1 0.1.9-1 all ASN.1 library for Python (Python 3 module)
ii python3-pyatspi 2.18.0+dfsg-3 all Assistive Technology Service Provider Interface - Python3 bindings
ii python3-pycurl 7.43.0-1ubuntu1 amd64 Python bindings to libcurl (Python 3)
ii python3-pyparsing 2.0.3+dfsg1-1ubuntu0.1 all Python parsing module, Python3 package
ii python3-renderpm 3.3.0-1 amd64 python low level render interface
ii python3-reportlab 3.3.0-1 all ReportLab library to create PDF documents using Python3
ii python3-reportlab-accel 3.3.0-1 amd64 C coded extension accelerator for the ReportLab Toolkit
ii python3-requests 2.9.1-3ubuntu0.1 all elegant and simple HTTP library for Python3, built for human beings
ii python3-six 1.10.0-3 all Python 2 and 3 compatibility library (Python 3 interface)
ii python3-software-properties 0.96.20.9 all manage the repositories that you install software from
ii python3-speechd 0.8.3-1ubuntu3 all Python interface to Speech Dispatcher
ii python3-systemd 231-2build1 amd64 Python 3 bindings for systemd
ii python3-uno 1:5.1.6~rc2-0ubuntu1~xenial6 amd64 Python-UNO bridge
ii python3-update-manager 1:16.04.15 all python 3.x module for update-manager
ii python3-urllib3 1.13.1-2ubuntu0.16.04.2 all HTTP library with thread-safe connection pooling for Python3
ii python3-xdg 0.25-4 all Python 3 library to access freedesktop.org standards
ii python3-xkit 0.5.0ubuntu2 all library for the manipulation of xorg.conf files (Python 3)
ii python3-xlsxwriter 0.7.3-1 all Python 3 module for creating Excel XLSX files
ii python3.5 3.5.2-2ubuntu0~16.04.5~amd64 Minimal subset of the Python language (version 3.5)
ii python3.5-minimal 3.5.2-2ubuntu0~16.04.5 amd64 Minimal subset of the Python language (version 3.5)
ii qdbus 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus tool
ii qml-module-io-thp-pyotherside 1.4.0-2 amd64 asynchronous Python 3 Bindings for Qt 5 (QML plugin)
ii qml-module-qt-labs-folderlistmodel 5.5.1-2ubuntu6 amd64 Qt 5 folderlistmodel QML module
ii qml-module-qt-labs-settings 5.5.1-2ubuntu6 amd64 Qt 5 settings QML module
ii qml-module-qtfeedback 5.0~git20130529-0ubuntu13 amd64 Qt 5 Feedback QML module
ii qml-module-qtgraphicaleffects 5.5.1-1ubuntu1 amd64 Qt 5 Graphical Effects module
ii qml-module-qtquick-layouts 5.5.1-1ubuntu1 amd64 Qt 5 Quick Layouts QML module
ii qml-module-qtquick-window2 5.5.1-2ubuntu6 amd64 Qt 5 window 2 QML module
ii qml-module-qtquick2 5.5.1-2ubuntu6 amd64 Qt 5 Quick 2 QML module
ii qml-module-qtest 5.5.1-2ubuntu6 amd64 Qt 5 test QML module
ii qml-module-ubuntu-components 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Components QML plugin
ii qml-module-ubuntu-layouts 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Layouts QML plugin
ii qml-module-ubuntu-onlineaccounts 0.6+16.04.20151106-0ubuntu1 amd64 Expose the Online Accounts API to QML applications
ii qml-module-ubuntu-performancemetrics 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - PerformanceMetrics QML plugin
ii qml-module-ubuntu-test 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Test QML plugin
ii qml-module-ubuntu-web 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web QML module
ii qmlscene 5.5.1-2ubuntu6 amd64 Qt 5 QML scene viewer
ii qpdf 8.0.2-3~16.04.1 amd64 tools for transforming and inspecting PDF files
ii qt-at-spi 0.4.0-3 amd64 at-spi accessibility plugin for Qt
ii qtchooser 52-gae5eeef-2build1~gcc5.2 amd64 Wrapper to select between Qt development binary versions
ii qtcore4-110n 4:4.8.7+dfsg-5ubuntu2 all Qt 4 core module translations
ii qtdeclarative5-accounts-plugin 0.6+16.04.20151106-0ubuntu1 amd64 transitional dummy package for Online Accounts QML clients
ii qtdeclarative5-dev-tools 5.5.1-2ubuntu6 amd64 Qt 5 declarative development programs
ii qtdeclarative5-qtquick2-plugin 5.5.1-2ubuntu6 amd64 transitional dummy package Qt 5 Quick 2 QML module
ii qtdeclarative5-test-plugin 5.5.1-2ubuntu6 amd64 transitional dummy package for Qt 5 test QML module
ii qtdeclarative5-ubuntu-ui-toolkit-plugin 1.3.1918+16.04.20160404-0ubuntu1 amd64 Transitional dummy package for Ubuntu UI Toolkit
QML plugin
ii qtdeclarative5-unity-action-plugin 1.1.0+14.04.20140304-0ubuntu2~gcc5.1 amd64 Unity Action QML Components
ii qttranslations5-110n 5.5.1-2build1 all translations for Qt 5
ii readline-common 6.3-8ubuntu2 all GNU readline and history libraries, common files
ii remmina 1.1.2-3ubuntu1 amd64 remote desktop client for GNOME desktop environment
ii remmina-common 1.1.2-3ubuntu1 all common files for remmina remote desktop client
ii remmina-plugin-rdp 1:1.2-3ubuntu1 amd64 RDP plugin for remmina remote desktop client
ii remmina-plugin-vnc 1:1.2-3ubuntu1 amd64 VNC plugin for remmina remote desktop client
ii rename 0.20-4 all Perl extension for renaming multiple files
ii resolvconf 1.78ubuntu6 all name server information handler
ii rfkill 0.5-1ubuntu3.1 amd64 tool for enabling and disabling wireless devices
ii rythmbox 3.3-1ubuntu7 amd64 music player and organizer for GNOME
ii rythmbox-data 3.3-1ubuntu7 all data files for rythmbox
ii rythmbox-plugin-zeitgeist 3.3-1ubuntu7 all zeitgeist plugin for rythmbox music player
ii rythmbox-plugins 3.3-1ubuntu7 amd64 plugins for rythmbox music player
ii rsync 3.1.1-3ubuntu1.2 amd64 fast, versatile, remote (and local) file-copying tool
ii rsyslog 8.16.0-1ubuntu3 amd64 reliable system and kernel logging daemon
ii rtkit 0.11-4 amd64 Realtime Policy and Watchdog Daemon
ii samba 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 SMB/CIFS file, print, and login server for Unix
ii samba-common 2:4.3.11+dfsg-0ubuntu0.16.04.28 all common files used by both the Samba server and client

```

```

ii samba-common-bin 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Samba common files used by both the server and the client
ii samba-dsdb-modules 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Samba Directory Services Database
ii samba-libs 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Samba core libraries
ii samba-vfs-modules 2:4.3.11+dfsg-0ubuntu0.16.04.28 amd64 Samba Virtual FileSystem plugins
ii sane-utils 1.0.25+git20150528-0ubuntu2.16.04.1 amd64 API library for scanners -- utilities
ii sbsignitool 0.6~0ubuntu10.1 amd64 utility for signing and verifying files for UEFI Secure Boot
ii seahorse 3.18.0-2ubuntu1 amd64 GNOME front end for GnuPG
ii secureboot-db 1.4~0ubuntu0.16.04.1 amd64 Secure Boot updates for DB and DBX
ii sed 4.2.2-7 amd64 The GNU sed stream editor
ii sensible-utils 0.0.9ubuntu0.16.04.1 all Utilities for sensible alternative selection
ii session-migration 0.2.3 amd64 Tool to migrate in user session settings
ii session-shortcuts 1.2~0ubuntu0.16.04.1 all Allows you to shutdown, logout, and reboot from dash
ii sessioninstaller 0.20+bzr150~0ubuntu4.1 all APT based installer using PackageKit's session DBus API
ii sgml-base 1.26+mu4ubuntu1 all SGML infrastructure and SGML catalog file support
ii shared-mime-info 1.5-2ubuntu0.2 amd64 FreeDesktop.org shared MIME database and spec
ii shotwell 0.22.0+git20160108.r1.f2fb1f7-0ubuntu1.1 amd64 digital photo organizer
ii shotwell-common 0.22.0+git20160108.r1.f2fb1f7-0ubuntu1.1 all digital photo organizer - common files
ii signon-keyring-extension 0.6+14.10.20140513-0ubuntu2 amd64 GNOME keyring extension for signond
ii signon-plugin-oauth2 0.23+16.04.20151209-0ubuntu1 amd64 Single Signon oauth2 plugin
ii signon-plugin-password 8.58+16.04.20151125-0ubuntu1 amd64 Plain Password plugin for Single Sign On
ii signon-ui 0.17+16.04.20151125-0ubuntu1 all Dummy transitional package for signon-ui
ii signon-ui-service 0.17+16.04.20151125-0ubuntu1 all D-Bus service file for signon-ui
ii signon-ui-x11 0.17+16.04.20151125-0ubuntu1 amd64 Single Sign-on UI
ii signond 8.58+16.04.20151125-0ubuntu1 amd64 Single Sign On framework
ii simple-scan 3.20.0-0ubuntu1 amd64 Simple Scanning Utility
ii snapd 2.34.2~0ubuntu0.1 amd64 Daemon and tooling that enable snap packages
ii snapd-login-service 1.33~0ubuntu0.16.04.1 amd64 Daemon to allow non-root access to snapd
ii sni-gt 0.2.7+16.04.20170217.1-0ubuntu1 amd64 indicator support for Qt
ii software-properties-common 0.96.20.9 all manage the repositories that you install software from (common)
ii sound-theme-freedesktop 0.8-1 all freedesktop.org sound theme
ii speech-dispatcher 0.8.3-1ubuntu3 amd64 Common interface to speech synthesizers
ii speech-dispatcher-audio-plugins 0.8.3-1ubuntu3 amd64 Dispatcher: Audio output plugins
ii squashfs-tools 1:4.3-3ubuntu2.16.04.3 amd64 Tool to create and append to squashfs filesystems
ii ssh-import-id 5.5-0ubuntu1 all securely retrieve an SSH public key and install it locally
ii ssl-cert 1.0.37 all simple debconf wrapper for OpenSSL
ii strace 4.11-1ubuntu3 amd64 System call tracer
ii sudo 1.8.16~0ubuntu1.5 amd64 Provide limited super user privileges to specific users
ii suru-icon-theme 14.04+16.04.20180326-0ubuntu1 all Ubuntu Suru Icon theme
ii syslinux 3:6.03+dfsg-11ubuntu1 amd64 collection of bootloaders (DOS FAT and NTFS bootloader)
ii syslinux-common 3:6.03+dfsg-11ubuntu1 all collection of bootloaders (common)
ii syslinux-legacy 2:3.63+dfsg-2ubuntu8 amd64 Bootloader for Linux/i386 using MS-DOS floppies
ii system-config-printer-common 1.5.7+20160212-0ubuntu2 all Printer configuration GUI
ii system-config-printer-gnome 1.5.7+20160212-0ubuntu2 all Printer configuration GUI
ii system-config-printer-udev 1.5.7+20160212-0ubuntu2 amd64 Printer auto-configuration facility based on udev
ii systemd 229-4ubuntu21.16 amd64 system and service manager
ii systemd-sysv 229-4ubuntu21.16 amd64 system and service manager - SysV links
ii sysv-rc 2.88dsf-59.3ubuntu2 all System-V-like runlevel change mechanism
ii sysvinit-utils 2.88dsf-59.3ubuntu2 amd64 System-V-like utilities
ii t1utils 1.39-2 amd64 Collection of simple Type 1 font manipulation programs
ii tar 1.28-2.1ubuntu0.1 amd64 GNU version of the tar archiving utility
ii tcl 8.6.0+9 amd64 Tool Command Language (default version) - shell
ii tcl8.6 8.6.5+dfsg-2 amd64 Tcl (the Tool Command Language) v8.6 - shell
ii tcpcd 7.6.0-25 amd64 Wietse Venema's TCP wrapper utilities
ii tcpdump 4.9.2-0ubuntu0.16.04.1 amd64 command-line network traffic analyzer
ii tdb-tools 1.3.8-2 amd64 Trivial Database - bundled binaries
ii telnet 0.17-40 amd64 basic telnet client
ii thermald 1.5-2ubuntu4 amd64 Thermal monitoring and controlling daemon
ii thunderbird 1:60.5.1+build2-0ubuntu0.16.04.1 amd64 Email, RSS and newsgroup client with integrated spam filter
ii thunderbird-gnome-support 1:60.5.1+build2-0ubuntu0.16.04.1 amd64 Email, RSS and newsgroup client - GNOME support
ii thunderbird-locale-eh 1:60.5.1+build2-0ubuntu0.16.04.1 amd64 English language pack for Thunderbird
ii thunderbird-locale-en-us 1:60.5.1+build2-0ubuntu0.16.04.1 all Transitional English language pack for Thunderbird
ii time 1.7-25.1 amd64 GNU time program for measuring CPU resource usage
ii tk 8.6.0+9 amd64 Toolkit for Tcl and X11 (default version) - windowing shell
ii tk8.6 8.6.5-1 amd64 Tk toolkit for Tcl and X11 v8.6 - windowing shell
ii toshset 1.76-4 amd64 Access much of the Toshiba laptop hardware interface
ii totem 3.18.1-1ubuntu4 amd64 Simple media player for the GNOME desktop based on GStreamer
ii totem-common 3.18.1-1ubuntu4 all Data files for the Totem media player
ii totem-plugins 3.18.1-1ubuntu4 amd64 Plugins for the Totem media player
ii transmission-common 2.84-3ubuntu3.1 all lightweight BitTorrent client (common files)
ii transmission-gtk 2.84-3ubuntu3.1 amd64 lightweight BitTorrent client (GTK+ interface)
ii ttf-ancient-fonts-symbola 2.59-1 all symbolic font providing emoji characters from Unicode 7.0 (transitional package)
ii ttf-ubuntu-font-family 1:0.83-0ubuntu2 all Ubuntu Font Family, sans-serif typeface hinted for clarity
ii tzdata 2018i-0ubuntu0.16.04 all time zone and daylight-saving time data
ii ubuntu-advantage-tools 10ubuntu0.16.04.1 all management tools for Ubuntu Advantage
ii ubuntu-artwork 1:14.04+16.04.20180326-0ubuntu1 all Ubuntu themes and artwork
ii ubuntu-core-launcher 2.34.2ubuntu0.1 amd64 Transitional package for snapd
ii ubuntu-desktop 1.361.2 amd64 The Ubuntu desktop system
ii ubuntu-docs 16.04.4 all Ubuntu Desktop Guide
ii ubuntu-drivers-common 1:0.4.17.7 amd64 Detect and install additional Ubuntu driver packages
ii ubuntu-keyring 2012.05.19 all GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.361.2 amd64 Minimal core of Ubuntu
ii ubuntu-mobile-icons 14.04+16.04.20180326-0ubuntu1 all Ubuntu Mobile Icon theme
ii ubuntu-mono 14.04+16.04.20180326-0ubuntu1 all Ubuntu Mono Icon theme
ii ubuntu-release-upgrader-core 1:16.04.26 all manage release upgrades
ii ubuntu-release-upgrader-gtk 1:16.04.26 all manage release upgrades
ii ubuntu-session 3.18.1.2-1ubuntu1.16.04.2 all Ubuntu session
ii ubuntu-settings 15.10.8 all default settings for the Ubuntu desktop
ii ubuntu-software 3.20.5-0ubuntu0.16.04.11 amd64 Utility for browsing, installing, and removing software
ii ubuntu-sounds 0.13 all Ubuntu's GNOME audio theme
ii ubuntu-standard 1.361.2 amd64 The Ubuntu standard system
ii ubuntu-system-service 0.3 all Dbus service to set various system-wide configurations
ii ubuntu-touch-sounds 15.08 all sounds for the Ubuntu Touch image
ii ubuntu-ui-toolkit-theme 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Ubuntu Theme
ii ubuntu-wallpapers 16.04.1-0ubuntu1 all Ubuntu Wallpapers
ii ucf 3.0036 all Update Configuration File(s): preserve user changes to config files
ii udev 229-4ubuntu21.16 amd64 /dev/ and hotplug management daemon
ii udisks2 2.1.7-1ubuntu1 amd64 D-Bus service to access and manipulate storage devices

```

```

ii ufw 0.35-0ubuntu2 all program for managing a Netfilter firewall
ii unattended-upgrades 0.9ubuntu0.10 all automatic installation of security upgrades
ii unity 7.4.5+16.04.20180221-0ubuntu1 amd64 Interface designed for efficiency of space and interaction.
ii unity-accessibility-profiles 0.1.10-0ubuntu3 all Accessibility Profile Manager - Unity profile data
ii unity-asset-pool 0.8.24+15.04.20141217-0ubuntu2 all Unity Assets Pool
ii unity-control-center 15.04.0+16.04.20171130-0ubuntu1 amd64 utilities to configure the GNOME desktop
ii unity-control-center-faces 15.04.0+16.04.20171130-0ubuntu1 all utilities to configure the GNOME desktop - faces images
ii unity-control-center-signon 0.1.8+16.04.20160201-0ubuntu1 amd64 Unity Control Center extension for single signon
ii unity-greeter 16.04.2-0ubuntu1 amd64 Unity Greeter
ii unity-gtk-module-common 0.0.0+15.04.20150118-0ubuntu2 all Common files for GtkMenuShell D-Bus exporter
ii unity-gtk2-module 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell D-Bus exporter
ii unity-gtk3-module 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell D-Bus exporter
ii unity-lens-applications 7.1.0+16.04.20160701-0ubuntu1 amd64 Application lens for unity
ii unity-lens-files 7.1.0+16.04.20151217-0ubuntu1 amd64 File lens for unity
ii unity-lens-music 6.9.1+16.04-0ubuntu1 amd64 Music lens for unity
ii unity-lens-photos 1.0+14.04.20140318-0ubuntu1 all Photos lens for Unity
ii unity-lens-video 0.3.15+16.04.20160212.1-0ubuntu1 amd64 Unity Video lens
ii unity-schemas 7.4.5+16.04.20180221-0ubuntu1 all Interface designed for efficiency of space and interaction.
ii unity-scope-calculator 0.1+14.04.20140328-0ubuntu1 all Calculator scope for Unity
ii unity-scope-chromiumbookmarks 0.1+13.10.20130723-0ubuntu1 all Chromium bookmarks scope for Unity
ii unity-scope-colourlovers 0.1+13.10.20130723-0ubuntu1 all COLOURlovers scope for Unity
ii unity-scope-devhelp 0.1+14.04.20140328-0ubuntu1 all devhelp scope for Unity
ii unity-scope-firefoxbookmarks 0.1+13.10.20130809.1-0ubuntu1 all Firefox bookmarks scope for Unity
ii unity-scope-gdrive 0.9+16.04.20151125-0ubuntu1 all Google Drive scope for Unity
ii unity-scope-home 6.8.2+16.04.20160212.1-0ubuntu1 amd64 Home scope that aggregates results from multiple scopes
ii unity-scope-manpages 3.0+14.04.20140324-0ubuntu1 all Manual pages scope for Unity
ii unity-scope-openclipart 0.1+13.10.20130723-0ubuntu1 all OpenClipArt scope for Unity
ii unity-scope-texdoc 0.1+14.04.20140328-0ubuntu1 all Texdoc scope for Unity
ii unity-scope-tomboy 0.1+13.10.20130723-0ubuntu1 all Tomboy scope for Unity
ii unity-scope-video-remote 0.3.15+16.04.20160212.1-0ubuntu1 amd64 Remote Videos engine
ii unity-scope-virtualbox 0.1+13.10.20130723-0ubuntu1 all VirtualBox scope for Unity
ii unity-scope-yelp 0.1+13.10.20130723-0ubuntu1 all Help scope for Unity
ii unity-scope-zotero 0.1+13.10.20130723-0ubuntu1 all Zotero scope for Unity
ii unity-scopes-master-default 6.8.2+16.04.20160212.1-0ubuntu1 all Home scope that aggregates results from multiple scopes
ii unity-sscopes-runner 7.1.4+16.04.20180209.1-0ubuntu1 all desktop runner for misceallenous scopes
ii unity-services 7.4.5+16.04.20180221-0ubuntu1 amd64 Services for the Unity interface
ii unity-settings-daemon 15.04.0+16.04.20160701-0ubuntu3 amd64 daemon handling the Unity session settings
ii unity-webapps-common 2.4.17+15.10.20150616-0ubuntu2 all Unity WebApp integration scripts
ii unity-webapps-qml 0.1+16.04.20160114-0ubuntu1 amd64 Unity Webapps QML component
ii unity-webapps-service 2.5.0~+16.04.20160201-0ubuntu1 amd64 Service for Web Apps integration with the Unity desktop
ii uno-libs3 5.1.6~rc2-0ubuntu1-xenial6 amd64 LibreOffice UNO runtime environment -- public shared libraries
ii unzip 6.0-2ubuntu1 amd64 De-archiver for .zip files
ii update-inetd 4.43 all inedt configuration file updater
ii update-manager 1:16.04.15 all GNOME application that manages apt updates
ii update-manager-core 1:16.04.15 all manage release, upgrades
ii update-notifier 3.168.10 amd64 Daemon which notifies about package updates
ii update-notifier-common 3.168.10 all Files shared between update-notifier and other packages
ii upower 0.99.4-2ubuntu0.3 amd64 abstraction for power management
ii upstart 1.13.2-0ubuntu21.1 amd64 event-based init daemon - essential binaries
ii ure 5.1.6~rc2-0ubuntu1-xenial6 amd64 LibreOffice UNO runtime environment
ii ureadahead 0.100.0-19 amd64 Read required files in advance
ii usb-creator-common 0.3.2 amd64 create a startup disk using a CD or disc image (common files)
ii usb-creator-gtk 0.3.2 amd64 create a startup disk using a CD or disc image (for GNOME)
ii usb-modeswitch 2.2.5+repack0-1ubuntu1 amd64 mode switching tool for controlling "flip flop" USB devices
ii usb-modeswitch-data 20151101-1 all mode switching data for usb-modeswitch
ii usbmuxd 1.0.0-2 amd64 USB multiplexor daemon for iPhone and iPod Touch devices
ii usbutils 1:007-4 amd64 Linux USB utilities
ii util-linux 2.27.1-6ubuntu3.6 amd64 miscellaneous system utilities
ii uuid-runtime 2.27.1-6ubuntu3.6 amd64 runtime components for the Universally Unique ID library
ii vbetool 1.1-3 amd64 run real-mode video BIOS code to alter hardware state
ii vim 2:7.4.1689-3ubuntu1.4 amd64 Vi IMproved - enhanced vi editor
ii vim-common 2:7.4.1689-3ubuntu1.4 amd64 Vi IMproved - common files
ii vim-runtime 2:7.4.1689-3ubuntu1.4 all Vi IMproved - Runtime files
ii vim-tiny 2:7.4.1689-3ubuntu1.4 amd64 Vi IMproved - enhanced vi editor - compact version
ii vino 3.8.1-0ubuntu9.2 amd64 VNC server for GNOME
ii wamerican 7.1-1 all American English dictionary words for /usr/share/dict
ii wbritish 7.1-1 all British English dictionary words for /usr/share/dict
ii webapp-container 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web applications container
ii webbrowser-app 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web browser
ii wget 1.17.1-1ubuntu1.4 amd64 retrieves files from the web
ii whiptail 0.52.18-1ubuntu2 amd64 Displays user-friendly dialog boxes from shell scripts
ii whoopsie 0.2.5.5 amd64 Ubuntu error tracker submission
ii whoopsie-preferences 0.18 amd64 System preferences for error reporting
ii wireless-regdb 2018.05.09-0ubuntu1~16.04.1 all wireless regulatory database
ii wireless-tools 3.00~pre9-8ubuntu1 amd64 Tools for manipulating Linux Wireless Extensions
ii wpasupplicant 2.4-0ubuntu6.3 amd64 client support for WPA and WPA2 (IEEE 802.11i)
ii x11-apps 7.7+5+nmu1ubuntu1 amd64 X applications
ii x11-common 1:7.7+13ubuntu3.1 all X Window System (X.Org) infrastructure
ii x11-session-utils 7.7+2 amd64 X session utilities
ii x11-utils 7.7+3 amd64 X11 utilities
ii x11-xkb-utils 7.7+2 amd64 XKB utilities
ii x11-xserver-utils 7.7+2 amd64 X server utilities
ii xauth 1:1.0.9-1ubuntu2 amd64 X authentication utility
ii xbitmaps 1.1.1-2 all Base X bitmaps
ii xbrlapi 5.3.1-2ubuntu2.1 amd64 Access software for a blind person using a braille display - xbrlapi
ii xcursor-themes 1.0.4-1 all Base X cursor themes
ii xdg-user-dirs 0.15-2ubuntu6.16.04.1 amd64 tool to manage well known user directories
ii xdg-user-dirs-gtk 0.10-1ubuntu1 amd64 tool to manage well known user directories (Gtk extension)
ii xdg-utils 1.1.1-1ubuntu1.16.04.3 all desktop integration utilities from freedesktop.org
ii xdiagnose 3.8.4.1 all X.org diagnosis tool
ii xffonts-base 1:1.0.4+nmu1 all standard fonts for X
ii xffonts-encodings 1:1.0.4-2 all Encodings for X.Org fonts
ii xffonts-scalable 1:1.0.3-1.1 all scalable fonts for X
ii xffonts-utils 1:7.7+3ubuntu0.16.04.2 amd64 X Window System font utility programs
ii xinit 1.3.4-3ubuntu0.1 amd64 X server initialisation tool
ii xinput 1.6.2-1 amd64 Runtime configuration and test of XInput devices
ii xkb-data 2.16-1ubuntu1 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.13+nmu2 all XML infrastructure and XML Catalog file support
ii xorg 1:7.7+13ubuntu3.1 amd64 X.Org X Window System

```

```

ii xorg-docs-core 1:1.7.1-1ubuntu1_all Core documentation for the X.org X Window System
ii xserver-common 2:1.18.4-0ubuntu0.8 all common files used by various X servers
ii xserver-xorg-core-hwe-16.04 2:1.19.6-1ubuntu4.1~16.04.2 amd64 Xorg X server - core server
ii xserver-xorg-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X server
ii xserver-xorg-input-all-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X server -- input driver metapackage
ii xserver-xorg-input-evdev-hwe-16.04 1:2.10.5-1ubuntu1~16.04.1 amd64 X.Org X server -- evdev input driver
ii xserver-xorg-input-synaptics-hwe-16.04 1:9.0-1ubuntu1~16.04.1 amd64 Synaptics TouchPad driver for X.Org server
ii xserver-xorg-input-wacom-hwe-16.04 1:0.34.0-0ubuntu2~16.04.1 amd64 X.Org X server -- Wacom input driver
ii xserver-xorg-legacy-hwe-16.04 2:1.19.6-1ubuntu4.1~16.04.2 amd64 setuid root Xorg server wrapper
ii xserver-xorg-video-all-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X Server -- output driver metapackage
ii xserver-xorg-video-amdgpu-hwe-16.04 18.0.1-1~16.04.1 amd64 X.Org X server -- AMDGPU display driver
ii xserver-xorg-video-ati-hwe-16.04 1:18.0.1-1~16.04.1 amd64 X.Org X server -- AMD/ATI display driver wrapper
ii xserver-xorg-video-fbdev-hwe-16.04 1:0.4.4-1build6~16.04.1 amd64 X.Org X server -- fbdev display driver
ii xserver-xorg-video-intel-hwe-16.04 2:2.99.917+git20171229-1~16.04.1 amd64 X.Org X server -- Intel i8xx, i9xx display driver
ii xserver-xorg-video-nouveau-hwe-16.04 1:1.0.15-2~16.04.1 amd64 X.Org X server -- Nouveau display driver
ii xserver-xorg-video-qxl-hwe-16.04 0.1.5-2build1~16.04.1 amd64 X.Org X server -- QXL display driver
ii xserver-xorg-video-radeon-hwe-16.04 1:18.0.1-1~16.04.1 amd64 X.Org X server -- AMD/Radeon display driver
ii xserver-xorg-video-vesa-hwe-16.04 1:2.3.4-1build3~16.04.1 amd64 X.Org X server -- VESA display driver
ii xserver-xorg-video-vmware-hwe-16.04 1:13.2.1-1build1~16.04.1 amd64 X.Org X server -- VMware display driver
ii xterm 322-1ubuntu1 amd64 X terminal emulator
ii xul-ext-ubufox 3.4-0ubuntu0.16.04.2 all Ubuntu modifications for Firefox
ii xz-utils 5.1.1alpha+20120614-2ubuntu2 amd64 XZ-format compression utilities
ii yelp 3.18.1-1ubuntu4 amd64 Help browser for GNOME
ii yelp-xsl 3.18.1-1 all XSL stylesheets for the yelp help browser
ii zeitgeist-core 0.9.16-0ubuntu4 amd64 event logging framework - engine
ii zeitgeist-databus 0.9.16-0ubuntu4 amd64 event logging framework - passive logging daemon
ii zenity 3.18.1.1-1ubuntu2 amd64 Display graphical dialog boxes from shell scripts
ii zenity-common 3.18.1.1-1ubuntu2 all Display graphical dialog boxes from shell scripts (common files)
ii zip 3.0-11 amd64 Archiver for .zip files
ii zlib1g 1:1.2.8.2ubuntu4.1 amd64 compression library - runtime

```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute 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

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: 'daisa'
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: 'daisa'
Port: 22
Proto: SSH
Method: password

56468 - Time of Last System Startup**Synopsis**

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot system boot 4.15.0-45-generic Sat Nov 1 12:41 still running
reboot system boot 4.15.0-45-generic Tue Jul 21 05:29 - 05:45 {00:16}
reboot system boot 4.15.0-45-generic Mon Jul 20 22:25 - 22:30 {00:05}
reboot system boot 4.15.0-45-generic Mon Jul 20 21:11 - 22:21 {01:10}
reboot system boot 4.15.0-45-generic Mon Jul 20 19:16 - 22:21 {03:05}
reboot system boot 4.15.0-45-generic Mon Jul 20 19:04 - 22:21 {03:17}
reboot system boot 4.15.0-45-generic Thu Feb 28 18:15 - 18:16 {00:01}

wtmp begins Thu Feb 28 18:15:19 2019
```

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 10.84.42.33 to 10.84.42.93 :
10.84.42.33
10.84.42.93

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 : /lib/x86_64-linux-gnu/liblzma.so.5.0.0

Version : 5.1.1

Associated Package : liblzma5 5.1.1alpha

Confidence : High

Managed by OS : True

Version Source : Package

Path : /usr/bin/xz

Version : 5.1.1

Associated Package : xz-utils 5.1.1alpha

Confidence : High

Managed by OS : True

Version Source : Package

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

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm13

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

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 : rsync_3.1.1-3ubuntu1.2
- Fixed package : rsync_3.1.1-3ubuntu1.3+esm4

211732 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python regressions (USN-7015-6)

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-7015-6 advisory.

USN-7015-5 fixed vulnerabilities in python2.7. 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-7015-6>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:7015-6

Plugin Information

Published: 2024/11/22, Modified: 2024/11/22

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 : libpython2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm13
- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm13
- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm13
- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm13
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm13

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

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 : openssh-client_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-client_1:7.2p2-4ubuntu2.10+esm4
- Installed package : openssh-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-server_1:7.2p2-4ubuntu2.10+esm4
- Installed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10
- Fixed package : openssh-sftp-server_1:7.2p2-4ubuntu2.10+esm4

189907 - Ubuntu 16.04 ESM / 18.04 ESM : X.Org X Server regression (USN-6587-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6587-4 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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6587-4>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6587-4

Plugin Information

Published: 2024/02/01, Modified: 2024/10/29

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 : xserver-common_2:1.18.4-0ubuntu0.8
- Fixed package : xserver-common_2:1.18.4-0ubuntu0.12+esm10

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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-158-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

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 : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm3
- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm3

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

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 : snapd_2.34.2ubuntu0.1
- Fixed package : snapd_2.54.3+16.04.0ubuntu0.1~esm4

- Installed package : ubuntu-core-launcher_2.34.2ubuntu0.1
- Fixed package : ubuntu-core-launcher_2.54.3+16.04.0ubuntu0.1~esm4

178654 - Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel regression (USN-6191-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6191-1 advisory.

USN-6081-1, USN-6084-1, USN-6092-1 and USN-6095-1 fixed vulnerabilities in the Linux kernel.

Unfortunately, that update introduced a spurious warning in the IPv6 subsystem. This update removes the undesired warning message.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6191-1>

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:6191-1

Plugin Information

Published: 2023/07/20, 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 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-213-generic for this advisory.

165110 - Ubuntu 16.04 ESM / 18.04 LTS : poppler regression (USN-5606-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5606-2 advisory.

USN-5606-1 fixed a vulnerability in poppler. Unfortunately it was missing a commit to fix it properly.

This update provides the corresponding fix for Ubuntu 18.04 LTS and Ubuntu 16.04 ESM.

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-5606-2>**Solution**

Update the affected packages.

Risk Factor

None

References

XREF USN:5606-2

Plugin Information

Published: 2022/09/15, Modified: 2024/10/29

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 : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16+esm2
- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16+esm2
- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16+esm2

153781 - Ubuntu 16.04 ESM : Apache HTTP Server regression (USN-5090-4)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5090-4 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-5090-4>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5090-4

Plugin Information

Published: 2021/09/29, Modified: 2024/10/29

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 : apache2_2.4.18-2ubuntu3.15
- Fixed package : apache2_2.4.18-2ubuntu3.17+esm3
- Installed package : apache2-bin_2.4.18-2ubuntu3.15
- Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm3
- Installed package : apache2-data_2.4.18-2ubuntu3.15
- Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm3
- Installed package : apache2-utils_2.4.18-2ubuntu3.15
- Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm3

154431 - Ubuntu 16.04 ESM : Apport vulnerability (USN-5122-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5122-2 advisory.

USN-5122-1 fixed a vulnerability in Apport. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5122-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5122-2

Plugin Information

Published: 2021/10/26, Modified: 2024/10/29

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 : apport_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.30+esm3
- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.30+esm3
- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.30+esm3
- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.30+esm3

152957 - Ubuntu 16.04 ESM : NTFS-3G vulnerabilities (USN-5060-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5060-2 advisory.

USN-5060-1 fixed a vulnerability in NTFS-3G. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5060-2>

Solution

Update the affected ntfs-3g and / or ntfs-3g-dev packages.

Risk Factor

None

References

XREF USN:5060-2

Plugin Information

Published: 2021/09/01, Modified: 2024/10/29

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 : ntfs-3g 1:2015.3.14AR.1-1ubuntu0.1
- Fixed package : ntfs-3g 1:2015.3.14AR.1-1ubuntu0.3+esm1

153592 - Ubuntu 16.04 ESM : ca-certificates update (USN-5089-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5089-2 advisory.

USN-5089-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5089-2>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5089-2

Plugin Information

Published: 2021/09/23, Modified: 2024/10/29

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 : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_20210119~16.04.1ubuntu0.1~esm1

163110 - Ubuntu 16.04 ESM : ca-certificates update (USN-5473-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5473-2 advisory.

USN-5473-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5473-2>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5473-2

Plugin Information

Published: 2022/07/14, Modified: 2024/10/29

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 : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_20211016~16.04.1~esm1

168467 - Ubuntu 16.04 ESM : ca-certificates update (USN-5761-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5761-2 advisory.

USN-5761-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-5761-2>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:5761-2

Plugin Information

Published: 2022/12/07, Modified: 2024/10/29

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 : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_20211016~16.04.1~esm2

176336 - Ubuntu 16.04 ESM : ca-certificates update (USN-6105-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-6105-2 advisory.

USN-6105-1 updated ca-certificates. This provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://ubuntu.com/security/notices/USN-6105-2>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:6105-2

Plugin Information

Published: 2023/05/24, Modified: 2024/10/29

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 : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_20230311~16.04.1-esm1

153510 - Ubuntu 16.04 ESM : curl regression (USN-5079-4)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5079-4 advisory.

USN-5079-2 fixed vulnerabilities in curl. One of the fixes introduced 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-5079-4>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:5079-4

Plugin Information

Published: 2021/09/21, Modified: 2024/10/29

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 : libcurl3_7.47.0-1ubuntu2.12
- Fixed package : libcurl3_7.47.0-1ubuntu2.19+esm2

- Installed package : libcurl3-gnutls_7.47.0-1ubuntu2.12
- Fixed package : libcurl3-gnutls_7.47.0-1ubuntu2.19+esm2

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

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 : cups_2.1.3-4ubuntu0.7
- Fixed package : cups_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-bsd_2.1.3-4ubuntu0.7
- Fixed package : cups-bsd_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-client_2.1.3-4ubuntu0.7
- Fixed package : cups-client_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-common_2.1.3-4ubuntu0.7
- Fixed package : cups-common_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-core-drivers_2.1.3-4ubuntu0.7
- Fixed package : cups-core-drivers_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-daemon_2.1.3-4ubuntu0.7
- Fixed package : cups-daemon_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-ppdc_2.1.3-4ubuntu0.7
- Fixed package : cups-ppdc_2.1.3-4ubuntu0.11+esm7
- Installed package : cups-server-common_2.1.3-4ubuntu0.7
- Fixed package : cups-server-common_2.1.3-4ubuntu0.11+esm7
- Installed package : libcups2_2.1.3-4ubuntu0.7
- Fixed package : libcups2_2.1.3-4ubuntu0.11+esm7
- Installed package : libcupscgi1_2.1.3-4ubuntu0.7
- Fixed package : libcupscgi1_2.1.3-4ubuntu0.11+esm7
- Installed package : libcupsimage2_2.1.3-4ubuntu0.7
- Fixed package : libcupsimage2_2.1.3-4ubuntu0.11+esm7
- Installed package : libcupsmime1_2.1.3-4ubuntu0.7
- Fixed package : libcupsmime1_2.1.3-4ubuntu0.11+esm7
- Installed package : libcupsppdc1_2.1.3-4ubuntu0.7
- Fixed package : libcupsppdc1_2.1.3-4ubuntu0.11+esm7

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_2.20.1-0ubuntu2.18
- Fixed package : apport_2.20.1-0ubuntu2.27

- Installed package : apport-gtk_2.20.1-0ubuntu2.18
- Fixed package : apport-gtk_2.20.1-0ubuntu2.27

- Installed package : python3-apport_2.20.1-0ubuntu2.18
- Fixed package : python3-apport_2.20.1-0ubuntu2.27

- Installed package : python3-problem-report_2.20.1-0ubuntu2.18
- Fixed package : python3-problem-report_2.20.1-0ubuntu2.27
```

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_2.75-1ubuntu0.16.04.5
- Fixed package : dnsmasq-base_2.75-1ubuntu0.16.04.8

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_85.0.1+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_85.0.1+build1-0ubuntu0.16.04.1

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_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_81.0.2+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_81.0.2+build1-0ubuntu0.16.04.1

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

Plugin Information

Published: 2020/11/06, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_82.0.2+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_82.0.2+build1-0ubuntu0.16.04.1

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_3.20180807a.0ubuntu0.16.04.1
- Fixed package : intel-microcode_3.20201110.0ubuntu0.16.04.2

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

11/2/25, 1:18 AM

Photographer

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_20170717~16.04.2
- Fixed package : ca-certificates_20201027ubuntu0.16.04.1

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_20170717~16.04.2
- Fixed package : ca-certificates_20210119~16.04.1

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_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python-apt-common_1.1.0~beta1ubuntu0.16.04.11

- Installed package : python3-apt_1.1.0~beta1ubuntu0.16.04.2
- Fixed package : python3-apt_1.1.0~beta1ubuntu0.16.04.11

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_1.1.1-1ubuntu1.16.04.3
- Fixed package   : xdg-utils_1.1.1-1ubuntu1.16.04.5
```

183606 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regression (USN-4122-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4122-2 advisory.

USN-4122-1 fixed vulnerabilities in Firefox. The update caused a regression that resulted in a crash when changing YouTube playback speed 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-4122-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4122-2

Plugin Information

Published: 2023/10/20, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package   : firefox_69.0.2+build1-0ubuntu0.16.04.1
```

- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_69.0.2+build1-0ubuntu0.16.04.1

183636 - Ubuntu 16.04 LTS / 18.04 LTS : Firefox regressions (USN-4234-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4234-2 advisory.

USN-4234-1 fixed vulnerabilities in Firefox. The update introduced various minor regressions. This update fixes the problems.

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-4234-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4234-2

Plugin Information

Published: 2023/10/21, Modified: 2024/10/29

Plugin Output

tcp/0

- Installed package : firefox_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox_72.0.2+build1-0ubuntu0.16.04.1
- Installed package : firefox-locale-en_65.0.1+build2-0ubuntu0.16.04.1
- Fixed package : firefox-locale-en_72.0.2+build1-0ubuntu0.16.04.1

144112 - Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel regression (USN-4660-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4660-2 advisory.

USN-4660-1 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

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:4660-2

Plugin Information

Published: 2020/12/13, Modified: 2024/10/29

Plugin Output

tcp/0

Running Kernel level of 4.15.0-45-generic does not meet the minimum fixed level of 4.15.0-128-generic for this advisory.

147991 - Ubuntu 16.04 LTS / 18.04 LTS : Python regression (USN-4754-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4754-2 advisory.

USN-4754-1 fixed a vulnerability in Python. The fix for CVE-2021-3177 introduced a regression in Python 2.7. 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-4754-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4754-2

Plugin Information

Published: 2021/03/23, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libpython2.7-2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-2.7.12-1ubuntu0~16.04.16

- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.16

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.4
- Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.16
```

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7_2.7.12-1ubuntu0~16.04.16
- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.4
- Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.16

207800 - Ubuntu 16.04 LTS / 18.04 LTS : ca-certificates update (USN-7034-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7034-2 advisory.

USN-7034-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 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-7034-2>

Solution

Update the affected ca-certificates package.

Risk Factor

None

References

XREF USN:7034-2

Plugin Information

Published: 2024/09/26, Modified: 2024/09/26

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 : ca-certificates_20170717~16.04.2
- Fixed package : ca-certificates_202402031~16.04.1~esm1

143271 - Ubuntu 16.04 LTS / 18.04 LTS : poppler regression (USN-4646-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4646-2 advisory.

USN-4646-1 fixed vulnerabilities in poppler. The fix for CVE-2019-10871 introduced a regression causing certain applications linked against poppler to fail. This update backs out the 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-4646-2>

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:4646-2

Plugin Information

Published: 2020/11/26, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : libpoppler-glib8_0.41.0-0ubuntu1.12
- Fixed package : libpoppler-glib8_0.41.0-0ubuntu1.16

- Installed package : libpoppler58_0.41.0-0ubuntu1.12
- Fixed package : libpoppler58_0.41.0-0ubuntu1.16

- Installed package : poppler-utils_0.41.0-0ubuntu1.12
- Fixed package : poppler-utils_0.41.0-0ubuntu1.16
```

192022 - Ubuntu 16.04 LTS : OpenSSL update (USN-6663-2)**Synopsis**

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6663-2 advisory.

USN-6663-1 provided a security update for OpenSSL. This update provides the corresponding update for Ubuntu 16.04 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-6663-2>

Solution

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.

Risk Factor

None

References

XREF USN:6663-2

Plugin Information

Published: 2024/03/13, Modified: 2024/10/29

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

```
- Installed package : libssl1.0_0.1.0.2g-1ubuntu4.14
- Fixed package : libssl1.0_0.1.0.2g-1ubuntu4.20+esm12

- Installed package : openssl_1.0.2g-1ubuntu4.14
- Fixed package : openssl_1.0.2g-1ubuntu4.20+esm12
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.4 119728 4752 ? Ss 12:41 0:04 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 12:41 0:00 [kthreadd]
root 4 0.0 0.0 0 0 ? I< 12:41 0:00 [kworker/0:0H]
root 6 0.0 0.0 0 0 ? I< 12:41 0:00 [mm_percpu_wq]
root 7 0.3 0.0 0 0 ? S 12:41 0:35 [ksoftirqd/0]
root 8 0.0 0.0 0 0 ? I 12:41 0:02 [rcu_sched]
root 9 0.0 0.0 0 0 ? I 12:41 0:00 [rcu_bh]
root 10 0.0 0.0 0 0 ? S 12:41 0:00 [migration/0]
root 11 0.0 0.0 0 0 ? S 12:41 0:00 [watchdog/0]
root 12 0.0 0.0 0 0 ? S 12:41 0:00 [cpuhp/0]
root 13 0.0 0.0 0 0 ? S 12:41 0:00 [kdevtmpfs]
root 14 0.0 0.0 0 0 ? I< 12:41 0:00 [netns]
root 15 0.0 0.0 0 0 ? S 12:41 0:00 [rcu_tasks_kthre]
root 16 0.0 0.0 0 0 ? S 12:41 0:00 [kauditfd]
root 17 0.0 0.0 0 0 ? S 12:41 0:00 [khungtaskd]
root 18 0.0 0.0 0 0 ? S 12:41 0:00 [oom_reaper]
root 19 0.0 0.0 0 0 ? I< 12:41 0:00 [writeback]
root 20 0.0 0.0 0 0 ? S 12:41 0:00 [kcompactd0]
root 21 0.0 0.0 0 0 ? SN 12:41 0:00 [ksmd]
root 22 0.0 0.0 0 0 ? SN 12:41 0:00 [khugepaged]
root 23 0.0 0.0 0 0 ? I< 12:41 0:00 [crypto]
root 24 0.0 0.0 0 0 ? I< 12:41 0:00 [kintegrityd]
root 25 0.0 0.0 0 0 ? I< 12:41 0:00 [kblockd]
root 26 0.0 0.0 0 0 ? I< 12:41 0:00 [ata_sff]
root 27 0.0 0.0 0 0 ? I< 12:41 0:00 [md]
root 28 0.0 0.0 0 0 ? I< 12:41 0:00 [edac-poller]
root 29 0.0 0.0 0 0 ? I< 12:41 0:00 [devfreq_wg]
root 30 0.0 0.0 0 0 ? I< 12:41 0:00 [watchdogd]
root 32 0.0 0.0 0 0 ? I 12:41 0:03 [kworker/0:1]
root 34 0.0 0.0 0 0 ? S 12:41 0:04 [kswapd0]
root 35 0.0 0.0 0 0 ? S 12:41 0:00 [ecryptfs-kthrea]
root 77 0.0 0.0 0 0 ? I< 12:41 0:00 [kthrotld]
root 78 0.0 0.0 0 0 ? I< 12:41 0:00 [acpi_thermal_pm]
root 79 0.0 0.0 0 0 ? S 12:41 0:00 [scsi_eh_0]
root 80 0.0 0.0 0 0 ? I< 12:41 0:00 [scsi_tmf_0]
root 81 0.0 0.0 0 0 ? S 12:41 0:00 [scsi_eh_1]
root 82 0.0 0.0 0 0 ? I< 12:41 0:00 [scsi_tmf_1]
root 88 0.0 0.0 0 0 ? I< 12:41 0:00 [ipv6_addrconf]
root 97 0.0 0.0 0 0 ? I< 12:41 0:00 [kstrt]
root 114 0.0 0.0 0 0 ? I< 12:41 0:00 [charger_manager]
root 167 0.0 0.0 0 0 ? I< 12:41 0:01 [kworker/0:1H]
root 168 0.0 0.0 0 0 ? S 12:41 0:00 [scsi_eh_2]
root 169 0.0 0.0 0 0 ? I< 12:41 0:00 [scsi_tmf_2]
root 170 0.0 0.0 0 0 ? I< 12:41 0:00 [ttm_swap]
root 171 0.0 0.0 0 0 ? S 12:41 0:00 [irq/18-vmwgfx]
root 194 0.0 0.0 0 0 ? S 12:41 0:00 [jbd2/sda1-8]
root 195 0.0 0.0 0 0 ? I< 12:41 0:00 [ext4-rsv-conver]
root 232 0.0 0.2 28448 2196 ? Ss 12:41 0:00 /lib/systemd/systemd-journald
root 263 0.0 0.1 45864 1348 ? Ss 12:41 0:00 /lib/systemd/systemd-udevd
root 279 0.0 0.0 0 0 ? I< 12:41 0:00 [ipt-VBoxWQqueue]
root 434 0.0 0.0 0 0 ? S 12:41 0:00 [jbd2/sda2-8]
root 436 0.0 0.0 0 0 ? I< 12:41 0:00 [ext4-rsv-conver]
```

```

root 441 0.0.0.0.0 ? S 12:41 0:00 [jbd2/sda4-8]
root 442 0.0.0.0.0 ? I< 12:41 0:00 [ext4-rsv-conver]
systemd+ 453 0.0.0.102384 968 ? Ssl 12:41 0:00 /lib/systemd/systemd-timesyncd
root 606 0.0.0.1 100340 768 ? Ss 12:41 0:00 /usr/sbin/cupsd -1
avahi 607 0.0.0.1 44904 1220 ? Ss 12:41 0:00 avahi-daemon: running [photographer.local]
root 610 0.0.0.3 298500 3308 ? Ssl 12:41 0:00 /usr/lib/accountsservice/accounts-daemon
root 618 0.0.0.2 28660 2304 ? Ss 12:41 0:00 /lib/systemd/systemd-logind
message+ 627 0.0.0.3 44252 3080 ? Ss 12:41 0:02 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nrepidfile --systemd-
activation
avahi 647 0.0.0.0 44788 28 ? S 12:41 0:00 avahi-daemon: chroot helper
root 650 0.0.0.1 274812 1924 ? Ssl 12:41 0:00 /usr/sbin/cups-browsed
root 651 0.0.0.3 462772 3916 ? Ssl 12:41 0:01 /usr/sbin/NetworkManager --no-daemon
root 652 0.0.0.0 4396 700 ? Ss 12:41 0:00 /usr/sbin/acpid
syslog 653 0.0.0.0 256396 804 ? Ssl 12:41 0:00 /usr/sbin/rsyslogd -n
root 654 0.0.0.1 36080 1568 ? Ss 12:41 0:00 /usr/sbin/cron -f
root 663 0.0.0.5 215332 5572 ? Ssl 12:41 0:00 /usr/lib/snapd/snapd
root 759 0.0.0.2 292204 2532 ? Sls 12:41 0:00 /usr/sbin/lightdm
root 790 0.0.0.5 304352 5476 ? Ssl 12:41 0:02 /usr/lib/policykit-1/polkitd --no-debug
root 829 0.1.1.9 369740 19412 tty7 Ssl+ 12:41 0:14 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten
tcp vt7 -nvtswitch
nobody 884 0.0.0.0 59936 224 ? S 12:41 0:00 /usr/sbin/dnsmasq --no-resolv --keep-in-foreground --no-hosts --bind-interfaces --pid-
file=/var/run/NetworkManager/dnsmasq.pid --listen-address=127.0.1.1 --cache-size=0 --conf-file=/dev/null --proxy-dnssec --enable-
dbus=org.freedesktop.NetworkManager.dnsmasq --conf-dir=/etc/NetworkManager/dnsmasq.d
root 1082 0.0.0.2 230308 2608 ? S1 12:41 0:00 lightdm --session-child 12 19
rtkit 1151 0.0.0.1 183548 1636 ? SNS 12:41 0:00 /usr/lib/rtkit/rtkit-daemon
root 1170 0.0.0.3 354216 3356 ? Ssl 12:41 0:00 /usr/lib/upower/upowerd
colord 1182 0.0.0.3 320540 3368 ? Ssl 12:41 0:00 /usr/lib/colord/colord
whoopsie 1193 0.0.0.3 452204 3068 ? Ssl 12:41 0:00 /usr/bin/whoopsie -f
root 1237 0.0.0.1 23004 1072 Ss+ 12:41 0:00 /sbin/agetty --noclear tty1 linux
root 1271 0.0.0.1 28236 1424 ? S 12:41 0:00 /bin/bash @usr/bin/mysqld_safe
root 1300 0.0.0.3 532468 3588 ? Ss 12:41 0:03 /usr/sbin/apache2 -k start
root 1435 0.0.0.2 247068 2368 ? Ss 12:41 0:00 /usr/sbin/nmbd -D
mysql 1459 0.0.1.8 600272 18168 ? S1 12:41 0:09 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib/mysql/plugin --user=mysql --skip-log-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock -
-port=3306
root 1460 0.0.0.0 33160 0 ? S 12:41 0:00 logger -t mysqld -p daemon error
root 1485 0.0.0.2 344976 2712 ? Ss 12:41 0:00 /usr/sbin/smbd -D
root 1486 0.0.0.0 336876 800 ? S 12:41 0:00 /usr/sbin/smbd -D
root 1488 0.0.0.0 344984 708 ? S 12:41 0:00 /usr/sbin/smbd -D
www-data 1774 0.0.0.6 533772 6116 ? S 13:37 0:02 /usr/sbin/apache2 -k start
www-data 1780 0.0.0.5 533736 5700 ? S 13:37 0:02 /usr/sbin/apache2 -k start
www-data 2160 0.0.0.0 4504 336 ? S 14:31 0:00 sh -c uname -a; w; id; /bin/sh -i
www-data 2164 0.0.0.0 4504 388 ? S 14:31 0:00 /bin/sh -i
www-data 2171 0.0.0.1 32480 1612 ? S 14:32 0:00 python -c import pty; pty.spawn("/bin/sh")
www-data 2172 0.0.0.0 4504 256 pts/8 Ss 14:32 0:00 /bin/sh
www-data 2173 0.0.0.1 32480 1492 pts/8 S+ 14:32 0:00 python -c import pty; pty.spawn("/bin/bash")
www-data 2174 0.0.0.1 18236 1504 pts/9 Ss+ 14:32 0:00 /bin/bash
root 2251 0.1 0.0.0 ? I 14:39 0:03 [kworker/0:0]
root 2294 0.0.0.0 16128 992 ? S 14:41 0:00 /sbin/dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf /var/run/dhclient-
enp0s3.pid -lf /var/lib/NetworkManager/dhclient-c26f8945-1916-37b3-8908-948299d18c71-enp0s3.lease -cf
/var/lib/NetworkManager/dhclient-enp0s3.conf enp0s3
www-data 2431 0.0.0.0 4504 284 ? S 14:45 0:00 sh -c uname -a; w; id; /bin/sh -i
www-data 2435 0.0.0.0 4504 344 ? S 14:45 0:00 /bin/sh -i
www-data 2441 0.0.0.1 36208 1628 ? S 14:46 0:00 python3 -c import pty; pty.spawn("/bin/bash")
www-data 2442 0.0.0.1 18236 1352 pts/10 Ss 14:46 0:00 /bin/bash
root 2445 0.0.0.0 0 ? I 14:46 0:00 [kworker/u2:1]
root 2453 0.0.0.1 343668 1624 pts/10 S+ 14:50 0:00 php7.2 -r posix_setuid(0); system('/bin/sh');
root 2454 0.0.0.0 4504 312 pts/10 S+ 14:50 0:00 sh -c /bin/sh
root 2455 0.0.0.0 4504 204 pts/10 S+ 14:50 0:00 /bin/sh
root 2489 0.0.0.0 0 ? I 14:55 0:00 [kworker/u2:3]
agi 2492 0.0.0.2 45284 2284 ? Ss 14:55 0:00 /lib/systemd/systemd --user
agi 2493 0.0.0.0 145272 268 ? S 14:55 0:00 (sd-pam)
agi 2517 0.0.0.1 212276 1032 ? S1 14:55 0:00 /usr/bin/gnome-keyring-daemon --daemonize --login
agi 2540 0.0.0.2 53540 2988 ? Ss 14:55 0:00 /sbin/upstart --user
agi 2620 0.0.0.1 39932 1288 ? S 14:55 0:00 upstart-udev-bridge --daemon --user
agi 2627 0.0.0.2 43728 2564 ? Ss 14:55 0:00 dbus-daemon --fork --session --address=unix:abstract=/tmp/dbus-azgkzhyewG
agi 2639 0.0.0.2 93416 2072 ? Ss 14:55 0:00 /usr/lib/x86_64-linux-gnu/hud/window-stack-bridge
agi 2669 0.0.0.0 39864 128 ? S 14:55 0:00 upstart-dbus-bridge --daemon --session --user --bus-name session
agi 2674 0.0.0.0 39864 132 ? S 14:55 0:00 upstart-dbus-bridge --daemon --system --user --bus-name system
agi 2675 0.0.0.1 48356 1204 ? S 14:55 0:00 upstart-file-bridge --daemon --user
agi 2688 0.0.0.6 532948 6904 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/bamf/bamfdaemon
agi 2691 0.0.0.2 365308 2288 ? Ssl 14:55 0:00 /usr/bin/ibus-daemon --daemonize --xim --address unix:tmpdir=/tmp/ibus
agi 2695 0.0.0.2 281588 2268 ? S1 14:55 0:00 /usr/lib/gvfs/gvfsd
agi 2706 0.0.0.2 419698 2128 ? S1 14:55 0:00 /usr/lib/gvfs/gvfsd-fuse /run/user/1001/gvfs -f -o big_writes
agi 2711 0.0.0.2 284628 2548 ? S1 14:55 0:00 /usr/lib/ibus/ibus-dconf
agi 2715 0.0.0.5 486716 5836 ? S1 14:55 0:00 /usr/lib/ibus/ibus-ui-gtk3
agi 2720 0.0.0.3 436992 3308 ? S1 14:55 0:00 /usr/lib/ibus/ibus-x11 --kill-daemon
agi 2724 0.0.0.2 353816 2176 ? S1 14:55 0:00 /usr/lib/at-spi2-core/at-spi-bus-launcher
agi 2731 0.0.0.1 42892 1500 ? S 14:55 0:00 /usr/bin/dbus-daemon --config-file=/etc/at-spi2/accessibility.conf --nofork --print-
address 3
agi 2738 0.0.0.2 206976 2524 ? S1 14:55 0:00 /usr/lib/at-spi2-core/at-spi2-registryd --use-gnome-session
agi 2750 0.0.0.2 208756 2056 ? S1 14:55 0:00 /usr/lib/ibus/ibus-engine-simple
agi 2754 0.0.0.1 173604 1748 ? Ss 14:55 0:00 gpg-agent --homedir /home/agi/.gnupg --use-standard-socket --daemon
agi 2764 0.0.0.2 653900 2992 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/hud/hud-service
agi 2766 0.0.0.6 937020 6492 ? Ssl 14:55 0:00 /usr/lib/unity-settings-daemon/unity-settings-daemon
agi 2776 0.0.0.3 560452 3416 ? Ssl 14:55 0:00 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
agi 2790 0.0.1.1 573216 11464 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/unity/unity-panel-service
agi 2825 0.0.0.2 178668 2476 ? S1 14:55 0:00 /usr/lib/dconf/dconf-service
agi 2828 0.0.0.3 377232 3864 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-messages/indicator-messages-service
agi 2829 0.0.0.2 356260 2128 ? S1 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-bluetooth/indicator-bluetooth-service
agi 2835 0.0.0.2 366592 2200 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-power/indicator-power-service
agi 2837 0.0.0.3 788908 3620 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-datetime/indicator-datetime-service
agi 2840 0.0.0.4 666616 4776 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-keyboard/indicator-keyboard-service --use-gtk
agi 2841 0.0.0.2 756552 2464 ? S1 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-sound/indicator-sound-service
agi 2845 0.0.0.3 556848 3796 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-printers/indicator-printers-service
agi 2849 0.0.0.2 643400 2456 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-session/indicator-session-service
agi 2856 0.0.0.2 403152 2492 ? Ssl 14:55 0:00 /usr/lib/x86_64-linux-gnu/indicator-application/indicator-application-service
agi 2884 0.0.0.2 637784 2452 ? S1 14:55 0:00 /usr/lib/evolution/evolution-source-registry
agi 2898 0.0.0.2 442028 2972 ? S<1 14:55 0:00 /usr/bin/pulseaudio --start --log-target=syslog

```

```

agi 2901 1.6 5.7 1240008 57800 ? Ss1 14:55 0:33 compiz
agi 2934 0.0 0.2 877012 2656 ? S1 14:55 0:00 /usr/lib/evolution/evolution-calendar-factory
agi 2949 0.0 0.5 672364 5728 ? S1 14:55 0:00 nm-applet
agi 2951 0.0 0.3 738108 3372 ? S1 14:55 0:00 nautilus -n
agi 2953 0.0 5.2 751624 53272 ? S1 14:55 0:00 /usr/bin/gnome-software --gapplication-service
agi 2960 0.0 0.2 303448 2160 ? S1 14:55 0:00 /usr/lib/gvfs/gvfs-udisks2-volume-monitor
agi 2967 0.0 0.6 646396 6976 ? S1 14:55 0:00 /usr/lib/polkit-gnome-authentication-agent-1
agi 2970 0.0 0.1 821696 1708 ? S1 14:55 0:00 /usr/lib/evolution/evolution-calendar-factory-subprocess --factory contacts --bus-name
org.gnome.evolution.dataserver.Subprocess.Backend.Calendarx2934x2 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/Calendar/2934/2
agi 2974 0.0 0.3 583992 3276 ? S1 14:55 0:00 /usr/lib/unity-settings-daemon/unity-fallback-mount-helper
root 2975 0.0 0.2 382392 2512 ? Ss1 14:55 0:00 /usr/lib/udisks2/udisksd --no-debug
agi 2996 0.0 0.1 264600 1840 ? S1 14:55 0:00 /usr/lib/gvfs/gvfs-goa-volume-monitor
agi 2997 0.0 0.1 814272 1820 ? S1 14:55 0:00 /usr/lib/evolution/evolution-calendar-factory-subprocess --factory local --bus-name
org.gnome.evolution.dataserver.Subprocess.Backend.Calendarx2934x3 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/Calendar/2934/3
agi 3002 0.0 0.2 704368 2428 ? S1 14:55 0:00 /usr/lib/evolution/evolution-addressbook-factory
agi 3016 0.0 0.1 266592 1272 ? S1 14:55 0:00 /usr/lib/gvfs/gvfs-ntp-volume-monitor
agi 3028 0.0 0.2 410684 2116 ? S1 14:55 0:00 /usr/lib/gvfs/gvfs-afc-volume-monitor
agi 3031 0.0 0.2 788068 2852 ? S1 14:55 0:00 /usr/lib/evolution/evolution-addressbook-factory-subprocess --factory local --bus-name
org.gnome.evolution.dataserver.Subprocess.Backend.AddressBookx3002x2 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/AddressBook/3002/2
agi 3040 0.0 0.1 278788 1392 ? S1 14:55 0:00 /usr/lib/gvfs/gphoto2-volume-monitor
root 3069 0.0 0.3 518404 3044 ? Ss1 14:55 0:00 /usr/lib/x86_64-linux-gnu/fwupd/fwupd
agi 3072 0.0 0.1 370740 1544 ? S1 14:55 0:00 /usr/lib/gvfsd-trash --spawner :1.5 /org/gtk/gvfs/exec_spaw/0
agi 3099 0.1 1.3 668600 14124 ? S1 14:55 0:02 /usr/lib/gnome-terminal/gnome-terminal-server
agi 3105 0.0 0.3 29488 3128 pts/6 Ss 14:55 0:00 bash
agi 3158 0.0 0.4 497956 4040 ? S1 14:56 0:00 zeitgeist-databus
agi 3165 0.0 0.0 4504 408 ? S 14:56 0:00 /bin/sh -c /usr/lib/x86_64-linux-gnu/zeitgeist/zeitgeist-maybe-vacuum; /usr/bin/zeitgeist-daemon
agi 3172 0.0 0.1 339972 1608 ? S1 14:56 0:00 /usr/bin/zeitgeist-daemon
agi 3180 0.0 0.2 310840 2504 ? S1 14:56 0:00 /usr/lib/x86_64-linux-gnu/zeitgeist-fts
agi 3195 0.0 0.2 193048 2480 ? S1 14:56 0:00 /usr/lib/gvfsd-metadata
agi 3233 0.0 0.6 458400 6672 ? S1 14:56 0:00 update-notifier
agi 3243 0.0 0.3 530304 3212 ? S1 14:57 0:00 /usr/lib/x86_64-linux-gnu/deja-dup/deja-dup-monitor
root 3254 0.0 0.1 61448 1852 pts/6 S 14:58 0:00 su daisa
daisa 3255 0.0 0.1 28272 1836 pts/6 S+ 14:58 0:00 bash
root 24348 0.0 0.2 65516 2942 ? Ss 14:59 0:00 /usr/sbin/sshd -D
agi 24421 0.0 0.8 579020 8316 ? S1 14:59 0:00 deja-dup --prompt
www-data 24902 0.1 1.7 533872 17908 ? S 15:17 0:00 /usr/sbin/apache2 -k start
www-data 25123 0.1 2.3 534020 23344 ? S 15:20 0:00 /usr/sbin/apache2 -k start
www-data 25230 0.2 1.8 533812 18380 ? S 15:22 0:00 /usr/sbin/apache2 -k start
root 25238 0.0 0.0 0 ? I 15:23 0:00 [kworker/u2:0]
www-data 25251 0.1 1.8 533940 18704 ? S 15:23 0:00 /usr/sbin/apache2 -k start
www-data 25255 0.1 1.7 533768 17844 ? S 15:23 0:00 /usr/sbin/apache2 -k start
www-data 25269 0.1 1.9 533976 19344 ? S 15:23 0:00 /usr/sbin/apache2 -k start
www-data 25273 0.2 2.3 534132 23464 ? S 15:23 0:00 /usr/sbin/apache2 -k start
root 25343 0.0 0.0 0 ? I 15:24 0:00 [kworker/0:2]
root 25351 0.0 0.0 0 ? I 15:24 0:00 [kworker/0:3]
root 25438 0.0 0.0 0 ? I 15:24 0:00 [kworker/0:4]
agi 25563 0.3 2.5 559164 26008 ? Ss1 15:24 0:00 /usr/lib/x86_64-linux-gnu/unity/unity-panel-service --lockscreen-mode
www-data 25622 0.2 2.2 533896 23008 ? S 15:25 0:00 /usr/sbin/apache2 -k start
root 25890 0.1 0.0 0 0 ? I 15:26 0:00 [kworker/0:5]
root 25929 0.0 0.0 0 ? I 15:27 0:00 [kworker/u2:2]
www-data 25968 0.1 1.6 533660 16332 ? S 15:27 0:00 /usr/sbin/apache2 -k start
www-data 26059 0.0 1.2 533236 12704 ? S 15:27 0:00 /usr/sbin/apache2 -k start
daisa 27177 0.2 0.4 45284 4616 ? Ss 15:28 0:00 /lib/systemd/systemd --user
daisa 27178 0.0 0.1 145272 1816 ? S 15:28 0:00 (sd-pam)
root 27451 0.3 0.6 94932 6720 ? Ss 15:28 0:00 sshd: daisa [priv]
root 27511 0.5 0.6 94932 6596 ? Ss 15:28 0:00 sshd: daisa [priv]
root 27520 0.5 0.6 94932 6784 ? Ss 15:28 0:00 sshd: daisa [priv]
daisa 27608 1.0 0.4 95104 4784 ? S 15:28 0:00 sshd: daisa@notty
daisa 27615 1.0 0.4 95104 4956 ? S 15:28 0:00 sshd: daisa@notty
daisa 27616 0.0 0.4 95104 4796 ? S 15:28 0:00 sshd: daisa@notty
daisa 27618 0.0 0.2 19580 2896 ? Ss 15:28 0:00 bash -c /bin/ps auxww 2>/dev/null
daisa 27619 0.0 0.3 44436 3284 ? R 15:28 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 : daisa

Protocol : SSH

189731 - Vim Installed (Linux)**Synopsis**

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

<https://www.vim.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of Vim:

Path : /usr/bin/vim.tiny
Version : 7.4

Path : /usr/bin/vim.basic
Version : 7.4

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

Can't connect to the 'root\CIMV2' WMI namespace.

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/8000/www

CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was :
http://10.84.42.93:8000/wiRSDq_vUova.html

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 :

PHOTOGRAPHER = Computer name
PHOTOGRAPHER = Messenger Service
PHOTOGRAPHER = 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.

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

Plugin Output

tcp/0

Nessus detected 2 installs of libcurl:

```
Path : /usr/lib/x86_64-linux-gnu/libcurl.so.4.4.0
Version : 7.47.0
Associated Package : libcurl3 7.47.0-1ubuntu2.12
Managed by OS : True

Path : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.4.0
Version : 7.47.0
Associated Package : libcurl3-gnutls 7.47.0-1ubuntu2.12
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 : /usr/lib/x86_64-linux-gnu/libexiv2.so.14.0.0
Version : 0.25
Associated Package : libexiv2-14 0.25-2.1ubuntu16.04.3
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 : photographer.local.

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 96% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4474-1): Update the affected packages.	159	1
Ubuntu 16.04 ESM : GNU binutils vulnerability (USN-5349-1): Update the affected packages.	150	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Thunderbird vulnerabilities (USN-4421-1): Update the affected packages.	93	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 ESM : Vim vulnerabilities (USN-5836-1): Update the affected packages.	64	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Firefox vulnerabilities (USN-4926-1): Update the affected packages.	60	1
Ubuntu 16.04 LTS / 18.04 LTS : ImageMagick vulnerabilities (USN-4192-1): Update the affected packages.	60	1
Ubuntu 14.04 LTS / 16.04 LTS : ImageMagick vulnerabilities (USN-7068-1): Update the affected packages.	55	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7121-1): Update the affected kernel package.	45	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 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-4394-1): Update the affected packages.	39	1
Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-6060-2): Update the affected packages.	38	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7185-1): Update the affected kernel package.	38	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7342-1): Update the affected kernel package.	38	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7069-1): Update the affected kernel package.	35	1
Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4637-2): Update the affected packages.	35	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Ghostscript vulnerabilities (USN-4469-1): Update the affected packages.	34	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7496-1): Update the affected kernel package.	33	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4094-1): 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 16.04 LTS / 18.04 LTS / 20.04 LTS : MySQL vulnerabilities (USN-4441-1): Update the affected packages.	30	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6926-1): Update the affected kernel package.	30	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4115-1): Update the affected kernel package.	28	1
Ubuntu 16.04 LTS / 18.04 LTS : tcpdump vulnerabilities (USN-4252-1): Update the affected tcpdump package.	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 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4287-1): Update the affected kernel package.	22	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7028-1): Update the affected kernel package.	22	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7428-1): Update the affected kernel package.	20	1
Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Exiv2 vulnerabilities (USN-5043-1): Update the affected packages.	20	1

Ubuntu 16.04 ESM : ImageMagick vulnerabilities (USN-5855-4): Update the affected packages.	20	1
Ubuntu 16.04 ESM : Linux kernel (HWE) vulnerabilities (USN-5883-1): Update the affected kernel package.	19	1
Ubuntu 16.04 ESM / 18.04 ESM : GNU binutils vulnerabilities (USN-6413-1): Update the affected packages.	18	1
Ubuntu 16.04 ESM : LibTIFF vulnerabilities (USN-5841-1): Update the affected packages.	18	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4418-1): Update the affected packages.	18	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6972-1): Update the affected kernel package.	18	1
Ubuntu 16.04 ESM / 18.04 LTS : ImageMagick vulnerabilities (USN-5736-1): Update the affected packages.	17	1
Ubuntu 16.04 ESM : Apache HTTP Server vulnerability (USN-5942-2): Update the affected packages.	17	1
Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5477-1): Update the affected packages.	17	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer vulnerabilities (USN-4434-1): Update the affected packages.	17	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6777-1): Update the affected kernel package.	17	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Python vulnerabilities (USN-4428-1): Update the affected packages.	16	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6740-1): Update the affected kernel package.	15	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 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7233-1): Update the affected kernel package.	15	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : NSS vulnerability (USN-4476-1): Update the affected packages.	14	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenLDAP vulnerability (USN-4744-1): Update the affected packages.	14	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4227-1): Update the affected kernel package.	14	1
Ubuntu 16.04 LTS : FreeRDP vulnerabilities (USN-4382-1): Update the affected packages.	14	1
Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6252-1): Update the affected kernel package.	13	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4979-1): Update the affected kernel package.	13	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5418-1): Update the affected kernel package.	13	1
Ubuntu 16.04 ESM : Apport vulnerabilities (USN-5077-2): Update the affected packages.	13	1
Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5560-2): Update the affected kernel package.	13	1
Ubuntu 16.04 LTS / 18.04 LTS : Ghostscript vulnerabilities (USN-7138-1): Update the affected packages.	13	1
Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4042-1): Update the affected packages.	13	1
Ubuntu 16.04 LTS : libsndfile vulnerability (USN-7267-1): Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.	13	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7627-1): Update the affected kernel package.	12	1
Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3931-2): Update the affected kernel package.	12	1
Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6440-1): Update the affected kernel package.	12	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5018-1): Update the affected kernel package.	12	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5298-1): Update the affected kernel package.	12	1
Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5778-2): Update the affected packages.	12	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4414-1): Update the affected kernel package.	12	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6701-1): Update the affected kernel package.	12	1

Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6866-1): Update the affected kernel package.	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 ESM : Linux kernel vulnerabilities (USN-5981-1): Update the affected kernel package.	11	1
Ubuntu 16.04 ESM : curl vulnerabilities (USN-5964-2): Update the affected packages.	11	1
Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2): 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 16.04 LTS / 18.04 LTS / 20.04 LTS : libexif vulnerabilities (USN-4396-1): Update the affected libexif-dev and / or libexif12 packages.	11	1
Ubuntu 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-4416-1): Update the affected packages.	11	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4185-1): Update the affected kernel package.	11	1
Ubuntu 16.04 LTS / 18.04 LTS : libsndfile vulnerabilities (USN-4013-1): Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.	11	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : BusyBox vulnerabilities (USN-3935-1): Update the affected packages.	10	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 ESM : X.Org X Server vulnerabilities (USN-6587-2): 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 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5515-1): Update the affected kernel package.	10	1
Ubuntu 16.04 ESM : Intel Microcode vulnerabilities (USN-5535-1): Update the affected intel-microcode package.	10	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Apport vulnerabilities (USN-4449-1): Update the affected packages.	10	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4162-1): Update the affected kernel package.	10	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4526-1): Update the affected kernel package.	10	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4660-1): Update the affected kernel package.	10	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7685-1): Update the affected kernel package.	10	1
Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6494-1): Update the affected kernel package.	9	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 ESM / 18.04 LTS / 20.04 LTS : libxml2 vulnerability (USN-5548-1): Update the affected packages.	9	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-4946-1): Update the affected kernel package.	9	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5136-1): Update the affected kernel package.	9	1
Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5768-1): Update the affected packages.	9	1
Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5669-2): Update the affected kernel package.	9	1
Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-5757-2): Update the affected kernel package.	9	1
Ubuntu 16.04 ESM : NTFS-3G vulnerability (USN-5711-2): Update the affected ntfs-3g and / or ntfs-3g-dev 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 16.04 LTS / 18.04 LTS / 20.04 LTS : Intel Microcode vulnerabilities (USN-4385-1): Update the affected intel-microcode package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenEXR vulnerabilities (USN-4900-1): Update the affected packages.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Exiv2 vulnerability (USN-4270-1): Update the affected exiv2, libexiv2-14 and / or libexiv2-dev packages.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4302-1): Update the affected kernel package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4345-1): Update the affected kernel package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4680-1): Update the affected kernel package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4749-1): Update the affected kernel package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7553-1): Update the affected kernel package.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerabilities (USN-7299-2): Update the affected packages.	9	1
Ubuntu 16.04 LTS / 18.04 LTS : elfutils vulnerabilities (USN-4012-1): Update the affected packages.	9	1
Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3981-2): Update the affected kernel package.	9	1
Ubuntu 16.04 ESM : Net-SNMP vulnerabilities (USN-5795-2): Update the affected packages.	8	1
Ubuntu 16.04 ESM : OpenSSL vulnerability (USN-6188-1): Update the affected libssl-dev, libssl1.0.0 and / or openssl packages.	8	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 : Bind vulnerabilities (USN-4468-1): Update the affected packages.	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 16.04 LTS / 18.04 LTS : LibTIFF vulnerabilities (USN-4158-1): Update the affected packages.	8	1
Ubuntu 16.04 LTS : Apport vulnerabilities (USN-6894-1): 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 ESM / 18.04 LTS : Apache HTTP Server regression (USN-5487-3): Update the affected packages.	7	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5466-1): Update the affected kernel package.	7	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5727-1): Update the affected kernel package.	7	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5790-1): Update the affected kernel package.	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 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerability (USN-4466-1): Update the affected packages.	7	1
Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-3): Update the affected packages.	7	1
Ubuntu 16.04 LTS / 18.04 LTS : LibRaw vulnerabilities (USN-3989-1): Update the affected packages.	7	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4578-1): Update the affected kernel package.	7	1
Ubuntu 16.04 LTS / 18.04 LTS : Qt vulnerabilities (USN-4275-1): Update the affected packages.	7	1

Ubuntu 16.04 LTS / 18.04 LTS : Thunderbird vulnerabilities (USN-4150-1): Update the affected packages.	7	1
Ubuntu 16.04 LTS / 18.04 LTS : wpa_supplicant and hostapd vulnerability (USN-4136-1): 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 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6342-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6396-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6604-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5094-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5209-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5339-1): Update the affected kernel package.	6	1
Ubuntu 16.04 ESM : Bind vulnerabilities (USN-5747-1): Update the affected packages.	6	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.	6	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : curl vulnerabilities (USN-4898-1): Update the affected packages.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : LibreOffice vulnerability (USN-4138-1): Update the affected packages.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4210-1): Update the affected kernel package.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4390-1): Update the affected kernel package.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4272-1): Update the affected packages.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : libsoup vulnerabilities (USN-7565-1): Update the affected packages.	6	1
Ubuntu 16.04 LTS / 18.04 LTS : libvpx vulnerabilities (USN-4199-1): Update the affected packages.	6	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libxml2 vulnerabilities (USN-7302-1): Update the affected packages.	5	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-6762-1): Update the affected packages.	5	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 ESM : GLib vulnerabilities (USN-6165-2): Update the affected packages.	5	1
Ubuntu 16.04 ESM / 18.04 ESM : Python vulnerabilities (USN-6513-1): 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 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5073-1): Update the affected kernel package.	5	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6029-1): Update the affected kernel package.	5	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6095-1): Update the affected kernel package.	5	1
Ubuntu 16.04 ESM : DjVuLibre vulnerabilities (USN-4957-2): Update the affected packages.	5	1
Ubuntu 16.04 ESM : OpenEXR vulnerabilities (USN-4996-2): Update the affected libopenexr-dev, libopenexr22 and / or openexr packages.	5	1
Ubuntu 16.04 ESM : Pillow vulnerabilities (USN-5227-2): Update the affected packages.	5	1

Ubuntu 16.04 ESM : Python vulnerability (USN-6394-1): 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 / 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 : Samba vulnerability (USN-4930-1): Update the affected packages.	5	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.	5	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libjpeg-turbo vulnerability (USN-4386-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : DjVuLibre vulnerabilities (USN-4198-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : GnuTLS vulnerabilities (USN-3999-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4376-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : file vulnerability (USN-4172-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : poppler vulnerabilities (USN-4646-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : systemd vulnerabilities (USN-4269-1): Update the affected packages.	5	1
Ubuntu 16.04 LTS / 18.04 LTS : unzip vulnerabilities (USN-4672-1): Update the affected unzip package.	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 / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.10 : Python vulnerabilities (USN-7488-1): Update the affected packages.	4	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Samba vulnerabilities (USN-7582-1): Update the affected 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 16.04 ESM / 18.04 ESM : LibTIFF vulnerabilities (USN-6229-1): Update the affected packages.	4	1
Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2): Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.	4	1
Ubuntu 16.04 ESM / 18.04 ESM : libx11 vulnerabilities (USN-6407-2): Update the affected 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 / 22.04 LTS : libxml2 vulnerabilities (USN-6028-1): Update the affected packages.	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 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5114-1): Update the affected kernel package.	4	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5268-1): Update the affected kernel package.	4	1

Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5385-1): Update the affected kernel package.	4	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-6130-1): Update the affected kernel package.	4	1
Ubuntu 16.04 ESM : CUPS vulnerability (USN-6128-2): Update the affected packages.	4	1
Ubuntu 16.04 ESM : Cairo vulnerabilities (USN-5407-1): Update the affected packages.	4	1
Ubuntu 16.04 ESM : Cron vulnerabilities (USN-5259-1): Update the affected cron package.	4	1
Ubuntu 16.04 ESM : DBD::mysql vulnerabilities (USN-5344-1): Update the affected libdbd-mysql-perl package.	4	1
Ubuntu 16.04 ESM : Ghostscript vulnerability (USN-5618-1): Update the affected packages.	4	1
Ubuntu 16.04 ESM : Libcroco vulnerabilities (USN-5389-1): Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.	4	1
Ubuntu 16.04 ESM : NSS vulnerability (USN-5892-2): Update the affected packages.	4	1
Ubuntu 16.04 ESM : Rsyslog vulnerability (USN-5404-2): Update the affected packages.	4	1
Ubuntu 16.04 ESM : libjpeg-turbo vulnerabilities (USN-5553-1): Update the affected packages.	4	1
Ubuntu 16.04 ESM : snapd vulnerabilities (USN-5292-3): Update the affected 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 / 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 : CUPS vulnerabilities (USN-4340-1): 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 16.04 LTS / 18.04 LTS : GVfs vulnerabilities (USN-4053-1): Update the affected packages.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : Libxslt vulnerabilities (USN-4164-1): Update the affected packages.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4363-1): Update the affected kernel package.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4426-1): Update the affected kernel package.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-4504-1): Update the affected packages.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : Pillow vulnerabilities (USN-4430-1): Update the affected packages.	4	1
Ubuntu 16.04 LTS / 18.04 LTS : rsync vulnerabilities (USN-4292-1): Update the affected rsync package.	4	1
Ubuntu 16.04 LTS : JasPer vulnerabilities (USN-4688-1): Update the affected libjasper-dev, libjasper-runtime and / or libjasper1 packages.	4	1
Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4068-2): Update the affected kernel package.	4	1
Ubuntu 16.04 LTS : zlib vulnerabilities (USN-4246-1): 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 : Jinja2 vulnerabilities (USN-7343-1): Update the affected python-jinja2 and / or python3-jinja2 packages.	3	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 14.04 LTS / 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3901-2): Update the affected kernel package.	3	1
Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 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 ESM : CUPS vulnerability (USN-6361-2): Update the affected packages.	3	1
Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerabilities (USN-6583-1): Update the affected packages.	3	1
Ubuntu 16.04 ESM / 18.04 ESM : OpenSSH vulnerabilities (USN-6560-2): Update the affected packages.	3	1
Ubuntu 16.04 ESM / 18.04 ESM : YAJL vulnerabilities (USN-6233-1): Update the affected libyajl-dev, libyajl2 and / or yajl-tools packages.	3	1
Ubuntu 16.04 ESM / 18.04 ESM : curl vulnerability (USN-6429-2): Update the affected packages.	3	1
Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : OpenSSL vulnerabilities (USN-6039-1): 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 : GD library vulnerabilities (USN-5068-1): Update the affected libgd-dev, libgd-tools and / or libgd3 packages.	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 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5003-1): Update the affected kernel package.	3	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5164-1): Update the affected kernel package.	3	1
Ubuntu 16.04 ESM : DHCP vulnerabilities (USN-5658-2): Update the affected packages.	3	1
Ubuntu 16.04 ESM : FriBidi vulnerabilities (USN-5922-1): Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 packages.	3	1
Ubuntu 16.04 ESM : Sudo vulnerabilities (USN-6005-2): Update the affected sudo and / or sudo-ldap packages.	3	1
Ubuntu 16.04 ESM : Vorbis vulnerabilities (USN-5420-1): Update the affected packages.	3	1
Ubuntu 16.04 ESM : X.Org X Server vulnerabilities (USN-5193-3): Update the affected packages.	3	1
Ubuntu 16.04 ESM : libXpm vulnerabilities (USN-5807-2): Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.	3	1
Ubuntu 16.04 ESM : libvpx vulnerabilities (USN-6403-3): Update the affected libvpx-dev, libvpx3 and / or vpx-tools packages.	3	1
Ubuntu 16.04 ESM : protobuf vulnerabilities (USN-5769-1): Update the affected 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 / 22.04 LTS : Python vulnerability (USN-7015-3): Update the affected packages.	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-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 : ImageMagick vulnerabilities (USN-4670-1): 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 : OpenLDAP vulnerability (USN-4352-1): Update the affected packages.	3	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : OpenSSL vulnerabilities (USN-4738-1): Update the affected packages.	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 : 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 : snapd vulnerabilities (USN-4424-1): 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 16.04 LTS / 18.04 LTS : Dnsmasq vulnerabilities (USN-6657-2): Update the affected packages.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4135-1): Update the affected kernel package.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4318-1): Update the affected kernel package.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4883-1): Update the affected kernel package.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6647-1): Update the affected kernel package.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : libarchive vulnerabilities (USN-4293-1): Update the affected packages.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : snapd vulnerabilities (USN-6940-2): Update the affected packages.	3	1
Ubuntu 16.04 LTS / 18.04 LTS : urllib3 vulnerabilities (USN-3990-1): Update the affected python-urllib3 and / or python3-urllib3 packages.	3	1
Ubuntu 16.04 LTS : GNU C Library vulnerability (USN-7259-2): Update the affected packages.	3	1
JQuery 1.2 < 3.5.0 Multiple XSS: Upgrade to JQuery version 3.5.0 or later.	2	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 / 16.04 LTS / 18.04 LTS : Bind vulnerabilities (USN-6723-1): Update the affected packages.	2	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Firefox vulnerabilities (USN-3919-1): Update the affected packages.	2	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GD vulnerabilities (USN-3900-1): Update the affected packages.	2	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Wget vulnerabilities (USN-3943-1): Update the affected wget and / or wget-udeb 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 / 23.10 : Jinja2 vulnerabilities (USN-6599-1): Update the affected python-jinja2 and / or python3-jinja2 packages.	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 ESM : Bind vulnerability (USN-6421-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM / 18.04 ESM : BusyBox vulnerabilities (USN-6335-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM / 18.04 ESM : OpenSSL vulnerabilities (USN-6435-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM / 18.04 ESM : libssh vulnerabilities (USN-6592-2): 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 : Linux kernel vulnerabilities (USN-5443-1): Update the affected kernel package.	2	1
Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PCRE vulnerabilities (USN-5425-1): 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 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5044-1): Update the affected kernel package.	2	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5319-1): Update the affected kernel package.	2	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerabilities (USN-5621-1): Update the affected kernel package.	2	1
Ubuntu 16.04 ESM / 18.04 LTS : OpenEXR vulnerability (USN-5150-1): Update the affected libopenexr-dev, libopenexr22 and / or openexr packages.	2	1
Ubuntu 16.04 ESM / 18.04 LTS : shadow vulnerabilities (USN-5254-1): Update the affected login, passwd and / or uidmap packages.	2	1
Ubuntu 16.04 ESM : BlueZ vulnerabilities (USN-4989-2): Update the affected packages.	2	1
Ubuntu 16.04 ESM : DBus vulnerability (USN-6372-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM : GPT fdisk vulnerabilities (USN-5262-1): Update the affected gdisk package.	2	1
Ubuntu 16.04 ESM : Libgcrypt vulnerabilities (USN-5080-2): Update the affected libgcrypt11-dev, libgcrypt20 and / or libgcrypt20-dev packages.	2	1
Ubuntu 16.04 ESM : Libtasn1 vulnerability (USN-5707-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM : Libxslt vulnerabilities (USN-5575-2): Update the affected packages.	2	1
Ubuntu 16.04 ESM : PCRE vulnerabilities (USN-5665-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM : Perl DBI module vulnerabilities (USN-5030-2): Update the affected libdbi-perl package.	2	1
Ubuntu 16.04 ESM : QPDF vulnerabilities (USN-5026-2): Update the affected libqpdf-dev, libqpdf21 and / or qpdf packages.	2	1
Ubuntu 16.04 ESM : SQLite vulnerability (USN-5712-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM : Squashfs-Tools vulnerabilities (USN-5078-2): Update the affected squashfs-tools package.	2	1
Ubuntu 16.04 ESM : jbig2dec vulnerabilities (USN-5405-1): Update the affected jbig2dec, libjbig2dec0 and / or libjbig2dec0-dev packages.	2	1
Ubuntu 16.04 ESM : libXi vulnerabilities (USN-5646-1): Update the affected libxi-dev and / or libxi6 packages.	2	1
Ubuntu 16.04 ESM : libXrandr vulnerabilities (USN-5428-1): Update the affected libxrandr-dev and / or libxrandr2 packages.	2	1
Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1): Update the affected libxrender-dev and / or libxrender1 packages.	2	1
Ubuntu 16.04 ESM : libcdio vulnerabilities (USN-5558-1): Update the affected packages.	2	1
Ubuntu 16.04 ESM : libpng vulnerabilities (USN-5432-1): Update the affected libpng12-0, libpng12-dev and / or libpng3 packages.	2	1

Ubuntu 16.04 ESM : libsndfile vulnerability (USN-5409-1): Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.	2	1
Ubuntu 16.04 ESM : libxml2 vulnerabilities (USN-5760-2): Update the affected packages.	2	1
Ubuntu 16.04 ESM : systemd vulnerabilities (USN-5013-2): Update the affected packages.	2	1
Ubuntu 16.04 ESM : tcpdump vulnerabilities (USN-5331-1): Update the affected tcpdump package.	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 : DBus vulnerability (USN-4398-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Evolution Data Server vulnerability (USN-4429-1): 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 : Python vulnerabilities (USN-4754-1): Update the affected 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 : libssh vulnerability (USN-4447-1): 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 : lxml vulnerability (USN-4896-1): Update the affected python-lxml and / or python3-lxml packages.	2	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.	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 16.04 LTS / 18.04 LTS : BlueZ vulnerabilities (USN-4311-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Expat vulnerability (USN-4132-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : File Roller vulnerability (USN-4332-1): Update the affected file-roller package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Firefox vulnerability (USN-4032-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : GD Graphics Library vulnerabilities (USN-4316-1): Update the affected libgd-dev, libgd-tools and / or libgd3 packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : GLib vulnerability (USN-4049-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Jinja2 vulnerabilities (USN-4011-1): Update the affected python-jinja2 and / or python3-jinja2 packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4017-1): Update the affected kernel package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4144-1): Update the affected kernel package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4877-1): Update the affected kernel package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4890-1): Update the affected kernel package.	2	1

Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4916-1): Update the affected kernel package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : OpenSSL vulnerabilities (USN-6632-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Patch vulnerabilities (USN-4071-1): Update the affected patch package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Perl DBI module vulnerability (USN-4534-1): Update the affected libdbi-perl package.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Python 2.7 vulnerability (USN-4754-4): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : Vim vulnerabilities (USN-4582-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : bzip2 vulnerabilities (USN-4038-1): Update the affected bzip2, libbz2-1.0 and / or libbz2-dev packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6718-2): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : e2fsprogs vulnerability (USN-4249-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : libbsd vulnerabilities (USN-4243-1): Update the affected libbsd-dev, libbsd0 and / or libbsd0-udeb packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : librsvg vulnerabilities (USN-4436-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : libxml2 vulnerabilities (USN-4274-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS / 18.04 LTS : python-apt vulnerabilities (USN-4247-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS : Bind vulnerabilities (USN-6909-3): Update the affected packages.	2	1
Ubuntu 16.04 LTS : BlueZ vulnerabilities (USN-7265-1): Update the affected packages.	2	1
Ubuntu 16.04 LTS : Dnsmasq vulnerabilities (USN-4924-1): Update the affected dnsmasq, dnsmasq-base and / or dnsmasq-utils packages.	2	1
Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-4255-2): Update the affected kernel package.	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 : Jinja2 vulnerability (USN-6787-1): Update the affected python-jinja2 and / or python3-jinja2 packages.	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 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PolicyKit vulnerability (USN-3934-1): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6944-2): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libvpx vulnerability (USN-7249-1): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libxml2 vulnerability (USN-6658-2): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ncurses vulnerability (USN-6684-1): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : poppler vulnerability (USN-3905-1): Update the affected packages.	1	1
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : systemd vulnerability (USN-3938-1): 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 libsndfile, 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 : Python vulnerability (USN-6139-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : AccountsService vulnerability (USN-6190-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : Apache HTTP Server vulnerability (USN-6510-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : Avahi vulnerability (USN-6129-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : FLAC vulnerability (USN-6360-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : Kerberos vulnerability (USN-6467-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : OpenLDAP vulnerability (USN-6197-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : Requests vulnerability (USN-6155-2): Update the affected python-requests and / or python3-requests packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : libcap2 vulnerability (USN-6166-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 ESM : ncurses vulnerability (USN-6451-1): 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 : 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 : lxml vulnerability (USN-5225-1): Update the affected python-lxml and / or python3-lxml 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 ESM / 18.04 LTS : Cron regression (USN-5259-3): Update the affected cron package.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : DjVuLibre vulnerability (USN-5005-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : GLib vulnerability (USN-5189-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : ICU vulnerability (USN-5133-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : Linux kernel vulnerability (USN-5357-1): Update the affected kernel package.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : Perl vulnerability (USN-6112-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : libICE vulnerability (USN-5744-1): Update the affected libice-dev and / or libice6 packages.	1	1
Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : APR vulnerability (USN-5056-1): Update the affected libapr1 and / or libapr1-dev packages.	1	1

Ubuntu 16.04 ESM : APR-util vulnerability (USN-5737-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Avahi vulnerability (USN-5008-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : BusyBox vulnerability (USN-5179-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Cyrus SASL vulnerability (USN-5301-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Dnsmasq vulnerability (USN-4976-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Expat vulnerability (USN-5638-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : FUSE vulnerability (USN-5326-1): Update the affected fuse, libfuse-dev and / or libfuse2 packages.	1	1
Ubuntu 16.04 ESM : FreeType vulnerability (USN-5453-1): Update the affected freetype2-demos, libfreetype6 and / or libfreetype6-dev packages.	1	1
Ubuntu 16.04 ESM : GCC vulnerability (USN-5770-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : GNU cpio vulnerability (USN-5064-2): Update the affected cpio package.	1	1
Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : GnuPG vulnerability (USN-5503-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : GnuTLS vulnerability (USN-5750-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Graphite2 vulnerability (USN-5657-1): Update the affected libgraphite2-3 and / or libgraphite2-dev packages.	1	1
Ubuntu 16.04 ESM : Gzip vulnerability (USN-5378-4): Update the affected gzip package.	1	1
Ubuntu 16.04 ESM : HTTP-Daemon vulnerability (USN-5520-2): Update the affected libhttp-daemon-perl package.	1	1
Ubuntu 16.04 ESM : HarfBuzz vulnerability (USN-5746-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : JACK vulnerability (USN-5656-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Jinja2 vulnerability (USN-5701-1): Update the affected python-jinja2 and / or python3-jinja2 packages.	1	1
Ubuntu 16.04 ESM : LZ4 vulnerability (USN-4968-2): Update the affected liblz4-1, liblz4-dev and / or liblz4-tool packages.	1	1
Ubuntu 16.04 ESM : Libksba vulnerability (USN-5787-2): Update the affected libksba-dev and / or libksba8 packages.	1	1
Ubuntu 16.04 ESM : Linux kernel vulnerability (USN-5591-1): Update the affected kernel package.	1	1
Ubuntu 16.04 ESM : OpenLDAP vulnerability (USN-5424-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : OpenSSH vulnerability (USN-5666-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : PolicyKit vulnerability (USN-5252-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : Samba vulnerability (USN-5260-3): Update the affected packages.	1	1
Ubuntu 16.04 ESM : WavPack vulnerability (USN-5721-1): Update the affected libwavpack-dev, libwavpack1 and / or wavpack packages.	1	1
Ubuntu 16.04 ESM : Wayland vulnerability (USN-5614-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : XZ Utils vulnerability (USN-5378-3): Update the affected packages.	1	1
Ubuntu 16.04 ESM : cups-filters vulnerability (USN-6083-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : libXdmcp vulnerability (USN-5690-1): Update the affected libxdmcp-dev and / or libxdmcp6 packages.	1	1
Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1): Update the affected libxfixes-dev and / or libxfixes3 packages.	1	1
Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1): Update the affected libxv-dev and / or libxv1 packages.	1	1

Ubuntu 16.04 ESM : libsamplerate vulnerability (USN-5749-1): Update the affected libsamplerate0, libsamplerate0-dev and / or samplerate-programs packages.	1	1
Ubuntu 16.04 ESM : libx11 vulnerability (USN-4966-2): Update the affected packages.	1	1
Ubuntu 16.04 ESM : man-db vulnerability (USN-5334-1): Update the affected man-db package.	1	1
Ubuntu 16.04 ESM : pixman vulnerability (USN-5718-2): Update the affected libpixman-1-0 and / or libpixman-1-dev packages.	1	1
Ubuntu 16.04 ESM : rsync vulnerability (USN-5359-2): Update the affected rsync package.	1	1
Ubuntu 16.04 ESM : util-linux vulnerability (USN-5478-1): Update the affected packages.	1	1
Ubuntu 16.04 ESM : zlib vulnerability (USN-5355-2): Update the affected 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

© 2025 Tenable™, Inc. All rights reserved.