Ubuntu – 192.168.217.131

Report generated by Tenable Nessus™ Sat, 28 Sep 2024 20:25:33 Egypt Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.217.130

16	111	52	6	66
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.217.130
MAC Address:	00:0C:29:09:9C:D7
OS:	Linux Kernel 5.4.0-84-generic on Ubuntu 18.04

Vulnerabilities

201456 - Canonical Ubuntu Linux SEoL (18.04.x)

Synopsis

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

Description

According to its version, Canonical Ubuntu Linux is 18.04.x. It is, therefore, no longer maintained by its vendor or provider.

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

See Also

https://ubuntu.com/blog/18-04-end-of-standard-support

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:C/I:C/A:C)

Plugin Information

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

Plugin Output

tcp/0

```
OS                                    : Canonical Ubuntu Linux 18.04.6 LTS (Bionic Beaver)
Security End of Life                  : May 30, 2023
Time since Security End of Life (Est.) : >= 1 year
```

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 meschanisms. 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)

VPR Score

7.1

EPSS Score

0.031

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 : libpython3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6_3.6.9-1~18.04ubuntu1.13+esm2

  - Installed package : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.13+esm2
```

```
  - Installed package : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.13+esm2

  - Installed package : python3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6_3.6.9-1~18.04ubuntu1.13+esm2

  - Installed package : python3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6-minimal_3.6.9-1~18.04ubuntu1.13+esm2
```

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)

VPR Score

6.7

EPSS Score

0.0152

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_2.0.4-9ubuntu2.2
  - Fixed package     : klibc-utils_2.0.4-9ubuntu2.2+esm1

  - Installed package : libklibc_2.0.4-9ubuntu2.2
  - Fixed package     : libklibc_2.0.4-9ubuntu2.2+esm1
```

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)

VPR Score

6.0

EPSS Score

0.0009

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_1.16-2ubuntu0.4
  - Fixed package     : krb5-locales_1.16-2ubuntu0.4+esm2

  - Installed package : libgssapi-krb5-2_1.16-2ubuntu0.4
  - Fixed package     : libgssapi-krb5-2_1.16-2ubuntu0.4+esm2

  - Installed package : libk5crypto3_1.16-2ubuntu0.4
  - Fixed package     : libk5crypto3_1.16-2ubuntu0.4+esm2

  - Installed package : libkrb5-3_1.16-2ubuntu0.4
  - Fixed package     : libkrb5-3_1.16-2ubuntu0.4+esm2

  - Installed package : libkrb5support0_1.16-2ubuntu0.4
  - Fixed package     : libkrb5support0_1.16-2ubuntu0.4+esm2
```

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)

VPR Score

6.7

EPSS Score

0.0009

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	IAVA:2024-A-0543
XREF	USN:7000-1

Plugin Information

Published: 2024/09/12, Modified: 2024/09/17

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 : libexpat1_2.2.5-3ubuntu0.9
  - Fixed package     : libexpat1_2.2.5-3ubuntu0.9+esm1
```

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

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

VPR Score

8.0

EPSS Score

0.0148

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

Plugin Information

Published: 2024/05/02, 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 : libc-bin_2.27-3ubuntu1.6
  - Fixed package     : libc-bin_2.27-3ubuntu1.6+esm2

  - Installed package : libc6_2.27-3ubuntu1.6
  - Fixed package     : libc6_2.27-3ubuntu1.6+esm2

  - Installed package : locales_2.27-3ubuntu1.6
  - Fixed package     : locales_2.27-3ubuntu1.6+esm2

  - Installed package : multiarch-support_2.27-3ubuntu1.6
  - Fixed package     : multiarch-support_2.27-3ubuntu1.6+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/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0077

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_1:1.27.2-2ubuntu3.4
  - Fixed package     : busybox-initramfs_1:1.27.2-2ubuntu3.4+esm1

  - Installed package : busybox-static_1:1.27.2-2ubuntu3.4
  - Fixed package     : busybox-static_1:1.27.2-2ubuntu3.4+esm1
```

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.

Original advisory details:

It was discovered that OpenSSH incorrectly handled loading certain PKCS#11

providers. If a user forwarded their ssh-agent to an untrusted system, a

remote attacker could possibly use this issue to load arbitrary libraries

from the user's system and execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6242-2

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/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)

VPR Score

6.7

EPSS Score

0.0582

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: 2024/09/19

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 : openssh-client_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-client_1:7.6p1-4ubuntu0.7+esm1

  - Installed package : openssh-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-server_1:7.6p1-4ubuntu0.7+esm1

  - Installed package : openssh-sftp-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-sftp-server_1:7.6p1-4ubuntu0.7+esm1
```

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)

VPR Score

6.7

EPSS Score

0.0021

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-2022-48565
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_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13+esm1

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13+esm1

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13+esm1
```

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.

Original advisory details:

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs. An

attacker could possibly use this issue to cause the X Server to crash,

obtain sensitive information, or execute arbitrary code. (CVE-2023-6816)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

reattaching to a different master device. An attacker could use this issue

to cause the X Server to crash, leading to a denial of service, or possibly

execute arbitrary code. (CVE-2024-0229)

Olivier Fourdan and Donn Seeley discovered that the X.Org X Server

incorrectly labeled GLX PBuffers when used with SELinux. An attacker could

use this issue to cause the X Server to crash, leading to a denial of

service. (CVE-2024-0408)

Olivier Fourdan discovered that the X.Org X Server incorrectly handled

the curser code when used with SELinux. An attacker could use this issue to

cause the X Server to crash, leading to a denial of service.

(CVE-2024-0409)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

memory when processing the XISendDeviceHierarchyEvent API. An attacker

could possibly use this issue to cause the X Server to crash, or execute

arbitrary code. (CVE-2024-21885)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

devices being disabled. An attacker could possibly use this issue to cause

the X Server to crash, or execute arbitrary code. (CVE-2024-21886)

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

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

See Also

https://ubuntu.com/security/notices/USN-6587-2

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)

VPR Score

6.7

EPSS Score

0.004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-6816
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: 2024/08/27

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 : xserver-common_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm4

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm4

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm4
```

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

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

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-2022-48624
XREF	USN:6664-1

Plugin Information

Published: 2024/02/27, 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 : less_487-0.1
  - Fixed package     : less_487-0.1ubuntu0.1~esm1
```

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.

Original advisory details:

It was discovered that Wget incorrectly handled semicolons in the userinfo

subcomponent of a URI. A remote attacker could possibly trick a user into

connecting to a different host than expected.

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

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

See Also

https://ubuntu.com/security/notices/USN-6852-2

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)

VPR Score

6.0

EPSS Score

0.0008

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: 2024/08/27

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 : wget_1.19.4-1ubuntu2.2
  - Fixed package     : wget_1.19.4-1ubuntu2.2+esm1
```

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

Synopsis

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

Description

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

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

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

CVE-2023-39353,

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

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

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

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

See Also

https://ubuntu.com/security/notices/USN-6401-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0035

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/0

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


  - Installed package : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm1

  - Installed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm1

  - Installed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm1
```

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

Synopsis

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

Description

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

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

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

(CVE-2022-3352, CVE-2022-4292)

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

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

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

(CVE-2022-3324)

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

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

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

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

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

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

See Also

https://ubuntu.com/security/notices/USN-6420-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0054

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-2022-3234
CVE	CVE-2022-3235
CVE	CVE-2022-3256
CVE	CVE-2022-3278
CVE	CVE-2022-3297
CVE	CVE-2022-3324
CVE	CVE-2022-3352
CVE	CVE-2022-3491

CVE	CVE-2022-3520
CVE	CVE-2022-3591
CVE	CVE-2022-3705
CVE	CVE-2022-4292
CVE	CVE-2022-4293
XREF	IAVB:2022-B-0049-S
XREF	IAVB:2022-B-0058-S
XREF	IAVB:2023-B-0016-S
XREF	USN:6420-1

Plugin Information

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

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm5

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm5

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm5
```

186677 - Ubuntu 18.04 ESM : FreeRDP vulnerabilities (USN-6522-2)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6522-2 advisory.

USN-6522-1 fixed several vulnerabilities in FreeRDP. This update provides the corresponding update for Ubuntu 18.04 LTS. Original advisory details:

It was discovered that FreeRDP incorrectly handled drive redirection. If a

user were tricked into connection to a malicious server, a remote attacker

could use this issue to cause FreeRDP to crash, resulting in a denial of

service, or possibly obtain sensitive information. (CVE-2022-41877)

It was discovered that FreeRDP incorrectly handled certain surface updates.

A remote attacker could use this issue to cause FreeRDP to crash, resulting

in a denial of service, or possibly execute arbitrary code.

(CVE-2023-39352, CVE-2023-39356)

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

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

See Also

https://ubuntu.com/security/notices/USN-6522-2

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)

VPR Score

6.7

EPSS Score

0.0031

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-2022-41877
CVE	CVE-2023-39352
CVE	CVE-2023-39356
XREF	USN:6522-2

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 : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libfreerdp-client2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm2

  - Installed package : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libfreerdp2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm2

  - Installed package : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.18.04.4
  - Fixed package     : libwinpr2-2_2.2.0+dfsg1-0ubuntu0.18.04.4+esm2
```

207057 - Ubuntu 18.04 LTS : Linux kernel vulnerabilities (USN-7003-2)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7003-2 advisory.

It was discovered that the JFS file system contained an out-of-bounds read vulnerability when printing xattr debug information. A local attacker could use this to cause a denial of service (system crash).

(CVE-2024-40902)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- MIPS architecture;

- PowerPC architecture;

- x86 architecture;

- ACPI drivers;

- Serial ATA and Parallel ATA drivers;

- Drivers core;

- GPIO subsystem;

- GPU drivers;

- Greybus drivers;

- HID subsystem;

- I2C subsystem;

- IIO subsystem;

- InfiniBand drivers;

- Media drivers;

- VMware VMCI Driver;

- Network drivers;

- Pin controllers subsystem;

- S/390 drivers;

- SCSI drivers;

- USB subsystem;

- JFFS2 file system;

- JFS file system;

- File systems infrastructure;

- NILFS2 file system;

- IOMMU subsystem;

- Sun RPC protocol;

- Netfilter;

- Memory management;

- B.A.T.M.A.N. meshing protocol;

- CAN network layer;

- Ceph Core library;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- IUCV driver;

- MAC80211 subsystem;

- NET/ROM layer;

- Network traffic control;

- SoC Audio for Freescale CPUs drivers; (CVE-2024-40941, CVE-2024-42086, CVE-2024-41097, CVE-2024-40958, CVE-2024-41089, CVE-2024-40942, CVE-2024-40968, CVE-2024-40934, CVE-2024-40902, CVE-2024-42124, CVE-2023-52887, CVE-2024-42115, CVE-2024-41041, CVE-2024-39501, CVE-2024-40932, CVE-2024-42102, CVE-2024-40960, CVE-2024-39487, CVE-2024-39503, CVE-2024-40945, CVE-2024-40959, CVE-2024-40987, CVE-2024-40995, CVE-2024-40988, CVE-2024-42084, CVE-2024-40943, CVE-2024-42070, CVE-2024-40904, CVE-2024-41049, CVE-2024-41046, CVE-2024-39502, CVE-2024-42097, CVE-2024-42090, CVE-2024-42236, CVE-2024-42223, CVE-2024-42094, CVE-2024-41007, CVE-2024-42105, CVE-2024-41035, CVE-2024-41087, CVE-2024-42157, CVE-2024-39495, CVE-2024-36894, CVE-2024-40916, CVE-2024-39469, CVE-2024-40974, CVE-2024-42153, CVE-2024-36974, CVE-2024-42096, CVE-2024-42232, CVE-2024-40980, CVE-2024-41034, CVE-2024-42087, CVE-2024-42093, CVE-2024-41095, CVE-2024-42145, CVE-2024-42148, CVE-2023-52803, CVE-2024-39499, CVE-2024-42104, CVE-2024-42224, CVE-2024-37078, CVE-2024-42092, CVE-2024-39505, CVE-2024-38619, CVE-2024-42106, CVE-2024-40978, CVE-2024-41044, CVE-2024-42089, CVE-2024-40981, CVE-2024-42154, CVE-2024-36978, CVE-2024-42076, CVE-2024-40984, CVE-2024-42127, CVE-2024-42119, CVE-2024-40961, CVE-2024-39509, CVE-2024-42101, CVE-2024-40901, CVE-2024-40963, CVE-2024-40905, CVE-2024-39506, CVE-2024-40912, CVE-2024-41006)

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

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

See Also

https://ubuntu.com/security/notices/USN-7003-2

Solution

Update the affected kernel package.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0038

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-52803
CVE	CVE-2023-52887
CVE	CVE-2024-36894
CVE	CVE-2024-36974
CVE	CVE-2024-36978
CVE	CVE-2024-37078
CVE	CVE-2024-38619
CVE	CVE-2024-39469
CVE	CVE-2024-39487
CVE	CVE-2024-39495
CVE	CVE-2024-39499

CVE	CVE-2024-39501
CVE	CVE-2024-39502
CVE	CVE-2024-39503
CVE	CVE-2024-39505
CVE	CVE-2024-39506
CVE	CVE-2024-39509
CVE	CVE-2024-40901
CVE	CVE-2024-40902
CVE	CVE-2024-40904
CVE	CVE-2024-40905
CVE	CVE-2024-40912
CVE	CVE-2024-40916
CVE	CVE-2024-40932
CVE	CVE-2024-40934
CVE	CVE-2024-40941
CVE	CVE-2024-40942
CVE	CVE-2024-40943
CVE	CVE-2024-40945
CVE	CVE-2024-40958
CVE	CVE-2024-40959
CVE	CVE-2024-40960
CVE	CVE-2024-40961
CVE	CVE-2024-40963
CVE	CVE-2024-40968
CVE	CVE-2024-40974
CVE	CVE-2024-40978
CVE	CVE-2024-40980
CVE	CVE-2024-40981
CVE	CVE-2024-40984
CVE	CVE-2024-40987
CVE	CVE-2024-40988
CVE	CVE-2024-40995
CVE	CVE-2024-41006
CVE	CVE-2024-41007
CVE	CVE-2024-41034
CVE	CVE-2024-41035
CVE	CVE-2024-41041
CVE	CVE-2024-41044
CVE	CVE-2024-41046
CVE	CVE-2024-41049
CVE	CVE-2024-41087
CVE	CVE-2024-41089
CVE	CVE-2024-41095

CVE	CVE-2024-41097
CVE	CVE-2024-42070
CVE	CVE-2024-42076
CVE	CVE-2024-42084
CVE	CVE-2024-42086
CVE	CVE-2024-42087
CVE	CVE-2024-42089
CVE	CVE-2024-42090
CVE	CVE-2024-42092
CVE	CVE-2024-42093
CVE	CVE-2024-42094
CVE	CVE-2024-42096
CVE	CVE-2024-42097
CVE	CVE-2024-42101
CVE	CVE-2024-42102
CVE	CVE-2024-42104
CVE	CVE-2024-42105
CVE	CVE-2024-42106
CVE	CVE-2024-42115
CVE	CVE-2024-42119
CVE	CVE-2024-42124
CVE	CVE-2024-42127
CVE	CVE-2024-42145
CVE	CVE-2024-42148
CVE	CVE-2024-42153
CVE	CVE-2024-42154
CVE	CVE-2024-42157
CVE	CVE-2024-42223
CVE	CVE-2024-42224
CVE	CVE-2024-42232
CVE	CVE-2024-42236
XREF	USN:7003-2

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.
```

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-195-generic
 for this advisory.
```

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

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

VPR Score

5.9

EPSS Score

0.0004

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-2024-36600
XREF	USN:6855-1

Plugin Information

Published: 2024/06/27, 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.


  - Installed package : libcdio17_1.0.0-2ubuntu2
  - Fixed package     : libcdio17_1.0.0-2ubuntu2+esm2
```

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)

VPR Score

6.5

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-32487
XREF	USN:6756-1

Plugin Information

Published: 2024/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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_487-0.1
  - Fixed package     : less_487-0.1ubuntu0.1~esm2
```

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

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)

VPR Score

6.7

EPSS Score

0.0004

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-2024-22667
XREF	USN:6698-1

Plugin Information

Published: 2024/03/18, 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 : vim-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm8

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm8

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm8
```

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)

VPR Score

6.7

EPSS Score

0.0005

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_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm7

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm7

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm7
```

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)

VPR Score

5.9

EPSS Score

0.0004

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-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_39.0.1-2ubuntu0.1
  - Fixed package     : python3-pkg-resources_39.0.1-2ubuntu0.1+esm1
```

190713 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 : LibTIFF vulnerabilities (USN-6644-1)

Synopsis

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

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6644-1 advisory.

It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the application to crash, resulting in a denial of service. (CVE-2023-52356)

It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-6228)

It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the application to consume resources, resulting in a denial of service. (CVE-2023-6277)

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

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

See Also

https://ubuntu.com/security/notices/USN-6644-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0012

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm5
```

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 icorrectly 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)

VPR Score

5.1

EPSS Score

0.05

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_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : bind9-host_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : dnsutils_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : dnsutils_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libbind9-160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libbind9-160_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libdns1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns1100_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libirs160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libirs160_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libisc-export169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc-export169_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libisc169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc169_1:9.11.3+dfsg-1ubuntu1.19+esm3
```

```
  - Installed package : libisccc160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccc160_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : libisccfg160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccfg160_1:9.11.3+dfsg-1ubuntu1.19+esm3

  - Installed package : liblwres160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : liblwres160_1:9.11.3+dfsg-1ubuntu1.19+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.

Original advisory details:

It was discovered that libxml2 incorrectly handled certain XML documents. A

remote attacker could possibly use this issue to cause libxml2 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-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)

VPR Score

4.4

EPSS Score

0.0005

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	IAVA:2024-A-0067
XREF	USN:6658-2

Plugin Information

Published: 2024/03/11, 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 : libxml2_2.9.4+dfsg1-6.1ubuntu1.9
  - Fixed package     : libxml2_2.9.4+dfsg1-6.1ubuntu1.9+esm1
```

205444 - Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS : Libcroco vulnerabilities (USN-6958-1)

Synopsis

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

Description

The remote Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6958-1 advisory.

It was discovered that Libcroco was incorrectly accessing data structures when reading bytes from memory, which could cause a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2017-7960)

It was discovered that Libcroco was incorrectly handling invalid UTF-8 values when processing CSS files.

An attacker could possibly use this issue to cause a denial of service. (CVE-2017-8834, CVE-2017-8871)

It was discovered that Libcroco was incorrectly implementing recursion in one of its parsing functions, which could cause an infinite recursion loop and a stack overflow due to stack consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-12825)

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

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

See Also

https://ubuntu.com/security/notices/USN-6958-1

Solution

Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0051

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-7960
CVE	CVE-2017-8834
CVE	CVE-2017-8871
CVE	CVE-2020-12825
XREF	USN:6958-1

Plugin Information

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

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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_0.6.12-2
  - Fixed package     : libcroco3_0.6.12-2ubuntu0.1~esm1
```

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)

VPR Score

5.0

EPSS Score

0.0014

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_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick_8:6.9.7.4+dfsg-16ubuntu6.15+esm2

  - Installed package : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15+esm2

  - Installed package : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15+esm2

  - Installed package : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm2

  - Installed package : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15+esm2

  - Installed package : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm2
```

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-2021-39212)

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)

VPR Score

6.7

EPSS Score

0.0039

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-2020-29599
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_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick_8:6.9.7.4+dfsg-16ubuntu6.15+esm1

  - Installed package : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15+esm1

  - Installed package : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15+esm1

  - Installed package : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm1

  - Installed package : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15+esm1

  - Installed package : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm1
```

185930 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Intel Microcode vulnerability (USN-6485-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6485-1 advisory.

Benoit Morgan, Paul Grosen, Thais Moreira Hamasaki, Ke Sun, Alyssa Milburn, Hisham Shafi, Nir Shlomovich, Tavis Ormandy, Daniel Moghimi, Josh Eads, Salman Qazi, Alexandra Sandulescu, Andy Nguyen, Eduardo Vela, Doug Kwan, and Kostik Shtoyk discovered that some Intel(R) Processors did not properly handle certain sequences of processor instructions. A local attacker could possibly use this to cause a core hang (resulting in a denial of service), gain access to sensitive information or possibly escalate their privileges.

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

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

See Also

https://ubuntu.com/security/notices/USN-6485-1

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/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)

VPR Score

7.4

EPSS Score

0.0004

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_3.20230214.0ubuntu0.18.04.1
  - Fixed package     : intel-microcode_3.20231114.0ubuntu0.18.04.1+esm1
```

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)

VPR Score

6.7

EPSS Score

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3896
CVE	CVE-2023-4733
CVE	CVE-2023-4734
CVE	CVE-2023-4735
CVE	CVE-2023-4738
CVE	CVE-2023-4750
CVE	CVE-2023-4751
CVE	CVE-2023-4752
CVE	CVE-2023-4781
CVE	CVE-2023-5344

CVE	CVE-2023-5441
CVE	CVE-2023-5535
XREF	IAVB:2023-B-0066-S
XREF	IAVB:2023-B-0074-S
XREF	USN:6452-1
XREF	IAVB:2023-B-0084-S
XREF	IAVA:2023-A-0579-S

Plugin Information

Published: 2023/10/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm6

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm6

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm6
```

186991 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6557-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6557-1 advisory.

It was discovered that Vim could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1725)

It was discovered that Vim could be made to recurse infinitely. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1771)

It was discovered that Vim could be made to write out of bounds with a put command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-1886)

It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1897, CVE-2022-2000)

It was discovered that Vim did not properly manage memory in the spell command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2042)

It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-46246, CVE-2023-48231)

It was discovered that Vim could be made to divide by zero. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-48232)

It was discovered that Vim contained multiple arithmetic overflows. An attacker could possibly use these issues to cause a denial of service. (CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237)

It was discovered that Vim did not properly manage memory in the substitute command. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-48706)

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

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

See Also

https://ubuntu.com/security/notices/USN-6557-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0018

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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm7

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm7

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm7
```

184303 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libsndfile vulnerability (USN-6471-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6471-1 advisory.

It was discovered that libsndfile contained multiple arithmetic overflows. If a user or automated system were tricked into processing a specially crafted audio file, an attacker could possibly use this issue to cause a denial of service.

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

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

See Also

https://ubuntu.com/security/notices/USN-6471-1

Solution

Update the affected libsndfile1, libsndfile1-dev and / or sndfile-programs packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-33065
XREF	USN:6471-1

Plugin Information

Published: 2023/11/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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_1.0.28-4ubuntu0.18.04.2
  - Fixed package     : libsndfile1_1.0.28-4ubuntu0.18.04.2+esm1
```

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)

VPR Score

6.0

EPSS Score

0.0009

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_1.22-1ubuntu0.18.04.2
  - Fixed package     : python3-urllib3_1.22-1ubuntu0.18.04.2+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/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/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0009

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_2.27-3ubuntu1.6
  - Fixed package     : libc-bin_2.27-3ubuntu1.6+esm1

  - Installed package : libc6_2.27-3ubuntu1.6
  - Fixed package     : libc6_2.27-3ubuntu1.6+esm1

  - Installed package : locales_2.27-3ubuntu1.6
  - Fixed package     : locales_2.27-3ubuntu1.6+esm1

  - Installed package : multiarch-support_2.27-3ubuntu1.6
  - Fixed package     : multiarch-support_2.27-3ubuntu1.6+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0015

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_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13

  - Installed package : libpython3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6_3.6.9-1~18.04ubuntu1.13

  - Installed package : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.13

  - Installed package : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.13

  - Installed package : python3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6_3.6.9-1~18.04ubuntu1.13

  - Installed package : python3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6-minimal_3.6.9-1~18.04ubuntu1.13
```

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)

VPR Score

6.7

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2426
CVE	CVE-2023-2609
CVE	CVE-2023-2610
XREF	USN:6154-1
XREF	IAVB:2023-B-0033-S
XREF	IAVB:2023-B-0035-S
XREF	IAVB:2023-B-0039-S

Plugin Information

Published: 2023/06/12, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm1

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm1

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm1
```

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 typahead.

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)

VPR Score

6.7

EPSS Score

0.0017

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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm3

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm3

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm3
```

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)

VPR Score

4.4

EPSS Score

0.0013

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_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler-glib8_0.62.0-2ubuntu2.14+esm2

  - Installed package : libpoppler73_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler73_0.62.0-2ubuntu2.14+esm2

  - Installed package : poppler-utils_0.62.0-2ubuntu2.14
  - Fixed package     : poppler-utils_0.62.0-2ubuntu2.14+esm2
```

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)

VPR Score

6.7

EPSS Score

0.001

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+0-0ubuntu0.18.04.18
  - Fixed package     : ghostscript_9.26~dfsg+0-0ubuntu0.18.04.18+esm2

  - Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : ghostscript-x_9.26~dfsg+0-0ubuntu0.18.04.18+esm2

  - Installed package : libgs9_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : libgs9_9.26~dfsg+0-0ubuntu0.18.04.18+esm2

  - Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : libgs9-common_9.26~dfsg+0-0ubuntu0.18.04.18+esm2
```

176745 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS : nghttp2 vulnerability (USN-6142-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6142-1 advisory.

Gal Goldshtein discovered that nghttp2 incorrectly handled certain inputs. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service.

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

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

See Also

https://ubuntu.com/security/notices/USN-6142-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0124

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-11080
XREF	USN:6142-1
XREF	CEA-ID:CEA-2021-0004

Plugin Information

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

Plugin Output

tcp/0

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


  - Installed package : libnghttp2-14_1.30.0-1ubuntu1
  - Fixed package     : libnghttp2-14_1.30.0-1ubuntu1+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.

Original advisory details:

Kevin Backhouse discovered that AccountsService incorrectly handled certain

D-Bus messages. A local attacker could use this issue to cause

AccountsService to crash, resulting in a denial of service, or possibly

execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6190-2

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)

VPR Score

6.7

EPSS Score

0.0004

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-2023-3297
XREF	USN:6190-2

Plugin Information

Published: 2023/09/25, 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 : accountsservice_0.6.45-1ubuntu1.3
  - Fixed package     : accountsservice_0.6.45-1ubuntu1.3+esm1

  - Installed package : gir1.2-accountsservice-1.0_0.6.45-1ubuntu1.3
  - Fixed package     : gir1.2-accountsservice-1.0_0.6.45-1ubuntu1.3+esm1

  - Installed package : libaccountsservice0_0.6.45-1ubuntu1.3
  - Fixed package     : libaccountsservice0_0.6.45-1ubuntu1.3+esm1
```

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.

Original advisory details:

Shoham Danino, Anat Bremler-Barr, Yehuda Afek, and Yuval Shavitt discovered

that Bind incorrectly handled the cache size limit. A remote attacker could

possibly use this issue to consume memory, leading to a denial of service.

(CVE-2023-2828)

It was discovered that Bind incorrectly handled the recursive-clients

quota. A remote attacker could possibly use this issue to cause Bind to

crash, resulting in a denial of service. This issue only affected Ubuntu

22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-2911)

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

Note that Nessus has not tested for 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)

VPR Score

4.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

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

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 : bind9-host_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : bind9-host_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : dnsutils_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : dnsutils_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libbind9-160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libbind9-160_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.18
```

```
  - Fixed package     : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libdns1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns1100_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libirs160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libirs160_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libisc-export169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc-export169_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libisc169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc169_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libisccc160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccc160_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : libisccfg160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccfg160_1:9.11.3+dfsg-1ubuntu1.19+esm1

  - Installed package : liblwres160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : liblwres160_1:9.11.3+dfsg-1ubuntu1.19+esm1
```

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/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0015

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_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : bind9-host_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : dnsutils_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : dnsutils_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libbind9-160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libbind9-160_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libdns1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns1100_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libirs160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libirs160_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libisc-export169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc-export169_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libisc169_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisc169_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libisccc160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccc160_1:9.11.3+dfsg-1ubuntu1.19+esm2

  - Installed package : libisccfg160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libisccfg160_1:9.11.3+dfsg-1ubuntu1.19+esm2
```

```
  - Installed package : liblwres160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : liblwres160_1:9.11.3+dfsg-1ubuntu1.19+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.

Original advisory details:

It was discovered that CUPS incorrectly handled certain memory operations.

An attacker could possibly use this issue to cause CUPS to crash, resulting

in a denial of service, or to possibly obtain sensitive information.

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

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

See Also

https://ubuntu.com/security/notices/USN-6184-2

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)

VPR Score

6.0

EPSS Score

0.0004

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: 2024/08/27

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_2.2.7-1ubuntu2.10
  - Fixed package     : cups_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-bsd_2.2.7-1ubuntu2.10
  - Fixed package     : cups-bsd_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-client_2.2.7-1ubuntu2.10
  - Fixed package     : cups-client_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-common_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-core-drivers_2.2.7-1ubuntu2.10
  - Fixed package     : cups-core-drivers_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-daemon_2.2.7-1ubuntu2.10
  - Fixed package     : cups-daemon_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-ipp-utils_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ipp-utils_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-ppdc_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ppdc_2.2.7-1ubuntu2.10+esm1

  - Installed package : cups-server-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-server-common_2.2.7-1ubuntu2.10+esm1

  - Installed package : libcups2_2.2.7-1ubuntu2.10
  - Fixed package     : libcups2_2.2.7-1ubuntu2.10+esm1
```

```
  - Installed package : libcupscgi1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupscgi1_2.2.7-1ubuntu2.10+esm1

  - Installed package : libcupsimage2_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsimage2_2.2.7-1ubuntu2.10+esm1

  - Installed package : libcupsmime1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsmime1_2.2.7-1ubuntu2.10+esm1

  - Installed package : libcupsppdc1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsppdc1_2.2.7-1ubuntu2.10+esm1
```

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.

Original advisory details:

It was discovered that CUPS incorrectly parsed certain Postscript objects.

If a user or automated system were tricked into printing a specially

crafted document, a remote attacker could use this issue to cause CUPS to

crash, resulting in a denial of service, or possibly execute arbitrary

code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6391-2

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)

VPR Score

6.7

EPSS Score

0.001

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: 2024/08/28

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 : cups_2.2.7-1ubuntu2.10
  - Fixed package     : cups_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-bsd_2.2.7-1ubuntu2.10
  - Fixed package     : cups-bsd_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-client_2.2.7-1ubuntu2.10
  - Fixed package     : cups-client_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-common_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-core-drivers_2.2.7-1ubuntu2.10
  - Fixed package     : cups-core-drivers_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-daemon_2.2.7-1ubuntu2.10
  - Fixed package     : cups-daemon_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-ipp-utils_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ipp-utils_2.2.7-1ubuntu2.10+esm2

  - Installed package : cups-ppdc_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ppdc_2.2.7-1ubuntu2.10+esm2
```

```
- Installed package : cups-server-common_2.2.7-1ubuntu2.10
- Fixed package     : cups-server-common_2.2.7-1ubuntu2.10+esm2

- Installed package : libcups2_2.2.7-1ubuntu2.10
- Fixed package     : libcups2_2.2.7-1ubuntu2.10+esm2

- Installed package : libcupscgi1_2.2.7-1ubuntu2.10
- Fixed package     : libcupscgi1_2.2.7-1ubuntu2.10+esm2

- Installed package : libcupsimage2_2.2.7-1ubuntu2.10
- Fixed package     : libcupsimage2_2.2.7-1ubuntu2.10+esm2

- Installed package : libcupsmime1_2.2.7-1ubuntu2.10
- Fixed package     : libcupsmime1_2.2.7-1ubuntu2.10+esm2

- Installed package : libcupsppdc1_2.2.7-1ubuntu2.10
- Fixed package     : libcupsppdc1_2.2.7-1ubuntu2.10+esm2
```

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.

Original advisory details:

It was discovered that FLAC incorrectly handled encoding certain files. A

remote attacker could use this issue to cause FLAC to crash, resulting in a

denial of service, or possibly execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6360-2

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)

VPR Score

6.7

EPSS Score

0.0009

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: 2024/08/27

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 : libflac8_1.3.2-1ubuntu0.1
  - Fixed package     : libflac8_1.3.2-1ubuntu0.1+esm1
```

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.

Original advisory details:

It was discovered that GLib incorrectly handled non-normal GVariants. An

attacker could use this issue to cause GLib to crash, resulting in a

denial of service, or perform other unknown attacks.

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

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

See Also

https://ubuntu.com/security/notices/USN-6165-2

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)

VPR Score

5.9

EPSS Score

0.0015

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: 2024/08/27

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_2.56.4-0ubuntu0.18.04.9
  - Fixed package     : libglib2.0-0_2.56.4-0ubuntu0.18.04.9+esm3

  - Installed package : libglib2.0-bin_2.56.4-0ubuntu0.18.04.9
  - Fixed package     : libglib2.0-bin_2.56.4-0ubuntu0.18.04.9+esm3

  - Installed package : libglib2.0-data_2.56.4-0ubuntu0.18.04.9
  - Fixed package     : libglib2.0-data_2.56.4-0ubuntu0.18.04.9+esm3
```

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)

VPR Score

6.7

EPSS Score

0.0015

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-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_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils_2.30-21ubuntu1~18.04.9+esm1

  - Installed package : binutils-common_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils-common_2.30-21ubuntu1~18.04.9+esm1
```

```
  - Installed package : binutils-x86-64-linux-gnu_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils-x86-64-linux-gnu_2.30-21ubuntu1~18.04.9+esm1

  - Installed package : libbinutils_2.30-21ubuntu1~18.04.9
  - Fixed package     : libbinutils_2.30-21ubuntu1~18.04.9+esm1
```

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)

VPR Score

6.7

EPSS Score

0.0061

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_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils_2.30-21ubuntu1~18.04.9+esm3

  - Installed package : binutils-common_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils-common_2.30-21ubuntu1~18.04.9+esm3

  - Installed package : binutils-x86-64-linux-gnu_2.30-21ubuntu1~18.04.9
  - Fixed package     : binutils-x86-64-linux-gnu_2.30-21ubuntu1~18.04.9+esm3

  - Installed package : libbinutils_2.30-21ubuntu1~18.04.9
  - Fixed package     : libbinutils_2.30-21ubuntu1~18.04.9+esm3
```

186613 - Ubuntu 16.04 ESM / 18.04 ESM : Open VM Tools vulnerabilities (USN-6463-2)

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-6463-2 advisory.

USN-6463-1 fixed vulnerabilities in Open VM Tools. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that Open VM Tools incorrectly handled SAML tokens. A

remote attacker with Guest Operations privileges could possibly use this

issue to elevate their privileges. (CVE-2023-34058)

Matthias Gerstner discovered that Open VM Tools incorrectly handled file

descriptors when dropping privileges. A local attacker could possibly use

this issue to hijack /dev/uinput and simulate user inputs. (CVE-2023-34059)

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

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

See Also

https://ubuntu.com/security/notices/USN-6463-2

Solution

Update the affected open-vm-tools, open-vm-tools-desktop and / or open-vm-tools-dev 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)

VPR Score

6.7

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-34058
CVE	CVE-2023-34059
XREF	USN:6463-2

Plugin Information

Published: 2023/12/06, 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 : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3+esm3

  - Installed package : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3+esm3
```

181838 - Ubuntu 16.04 ESM / 18.04 ESM : Open VM Tools vulnerability (USN-6365-2)

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-6365-2 advisory.

USN-6365-1 fixed a vulnerability in Open VM Tools. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that Open VM Tools incorrectly handled SAML tokens. A

remote attacker could possibly use this issue to bypass SAML token

signature verification and perform VMware Tools Guest Operations.

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

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

See Also

https://ubuntu.com/security/notices/USN-6365-2

Solution

Update the affected open-vm-tools, open-vm-tools-desktop and / or open-vm-tools-dev 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)

VPR Score

6.7

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-20900
XREF	USN:6365-2

Plugin Information

Published: 2023/09/25, 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 : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3+esm2

  - Installed package : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3+esm2
```

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)

VPR Score

4.4

EPSS Score

0.0044

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_2.4.45+dfsg-1ubuntu1.11
  - Fixed package     : libldap-2.4-2_2.4.45+dfsg-1ubuntu1.11+esm1

  - Installed package : libldap-common_2.4.45+dfsg-1ubuntu1.11
  - Fixed package     : libldap-common_2.4.45+dfsg-1ubuntu1.11+esm1
```

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.

Original advisory details:

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-6394-2

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)

VPR Score

4.4

EPSS Score

0.0009

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:6394-2

Plugin Information

Published: 2023/10/17, 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 : libpython2.7_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13+esm3

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13+esm3

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13+esm3
```

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.

Original advisory details:

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

prepending values to certain properties. An attacker could possibly use

this issue to cause the X Server to crash, execute arbitrary code, or

escalate privileges. (CVE-2023-5367)

Sri discovered that the X.Org X Server incorrectly handled detroying

windows in certain legacy multi-screen setups. An attacker could possibly

use this issue to cause the X Server to crash, execute arbitrary code, or

escalate privileges. (CVE-2023-5380)

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

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

See Also

https://ubuntu.com/security/notices/USN-6453-2

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)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5367
CVE	CVE-2023-5380
XREF	USN:6453-2

Plugin Information

Published: 2023/10/31, 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 : xserver-common_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm1

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm1

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm1
```

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.

Original advisory details:

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled XKB

button actions. An attacker could possibly use this issue to cause the X

Server to crash, execute arbitrary code, or escalate privileges.

(CVE-2023-6377)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

memory when processing the RRChangeOutputProperty and

RRChangeProviderProperty APIs. An attacker could possibly use this issue to

cause the X Server to crash, or obtain sensitive information.

(CVE-2023-6478)

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

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

See Also

https://ubuntu.com/security/notices/USN-6555-2

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)

VPR Score

6.7

EPSS Score

0.1598

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: 2024/08/28

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_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm3

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm3

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm3
```

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)

VPR Score

4.4

EPSS Score

0.0129

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_2.1.0-2build1
  - Fixed package     : libyajl2_2.1.0-2ubuntu0.18.04.1~esm1
```

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.

Original advisory details:

Yair Mizrahi discovered that libXpm incorrectly handled certain malformed

XPM image files. If a user were tricked into opening a specially crafted

XPM image file, a remote attacker could possibly use this issue to consume

memory, leading to a denial of service. (CVE-2023-43786)

Yair Mizrahi discovered that libXpm incorrectly handled certain malformed

XPM image files. If a user were tricked into opening a specially crafted

XPM image file, a remote attacker could use this issue to cause libXpm to

crash, leading to a denial of service, or possibly execute arbitrary code.

(CVE-2023-43787)

Alan Coopersmith discovered that libXpm incorrectly handled certain

malformed XPM image files. If a user were tricked into opening a specially

crafted XPM image file, a remote attacker could possibly use this issue to

cause libXpm to crash, leading to a denial of service. (CVE-2023-43788,

CVE-2023-43789)

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

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

See Also

https://ubuntu.com/security/notices/USN-6408-2

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)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-43786
CVE	CVE-2023-43787
CVE	CVE-2023-43788
CVE	CVE-2023-43789
XREF	USN:6408-2

Plugin Information

Published: 2023/10/23, 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 : libxpm4_1:3.5.12-1ubuntu0.18.04.2
```

```
  - Fixed package     : libxpm4_1:3.5.12-1ubuntu0.18.04.2+esm1
```

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.

Original advisory details:

Richard Weinberger discovered that libcap2 incorrectly handled certain long

input strings. An attacker could use this issue to cause libcap2 to crash,

resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2023-2603)

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

Note that Nessus has not tested for 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/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)

VPR Score

6.7

EPSS Score

0.0004

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-2023-2603
XREF	USN:6166-2

Plugin Information

Published: 2023/06/19, 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 : libcap2_1:2.25-1.2
  - Fixed package     : libcap2_1:2.25-1.2ubuntu0.1~esm1

  - Installed package : libcap2-bin_1:2.25-1.2
  - Fixed package     : libcap2-bin_1:2.25-1.2ubuntu0.1~esm1

  - Installed package : libpam-cap_1:2.25-1.2
  - Fixed package     : libpam-cap_1:2.25-1.2ubuntu0.1~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.

Original advisory details:

Gregory James Duck discovered that libx11 incorrectly handled certain

keyboard symbols. If a user were tricked into connecting to a malicious X

server, a remote attacker could use this issue to cause libx11 to crash,

resulting in a denial of service, or possibly execute arbitrary code.

(CVE-2023-43785)

Yair Mizrahi discovered that libx11 incorrectly handled certain malformed

XPM image files. If a user were tricked into opening a specially crafted

XPM image file, a remote attacker could possibly use this issue to consume

memory, leading to a denial of service. (CVE-2023-43786)

Yair Mizrahi discovered that libx11 incorrectly handled certain malformed

XPM image files. If a user were tricked into opening a specially crafted

XPM image file, a remote attacker could use this issue to cause libx11 to

crash, leading to a denial of service, or possibly execute arbitrary code.

(CVE-2023-43787)

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

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

See Also

https://ubuntu.com/security/notices/USN-6407-2

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)

VPR Score

6.7

EPSS Score

0.0004

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: 2024/08/27

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 : libx11-6_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-6_2:1.6.4-3ubuntu0.4+esm2
```

```
  - Installed package : libx11-data_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-data_2:1.6.4-3ubuntu0.4+esm2

  - Installed package : libx11-xcb1_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-xcb1_2:1.6.4-3ubuntu0.4+esm2
```

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.

Original advisory details:

Gregory James Duck discovered that libx11 incorrectly handled certain

Request, Event, or Error IDs. If a user were tricked into connecting to a

malicious X Server, a remote attacker could possibly use this issue to

cause libx11 to crash, resulting in a denial of service.

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

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

See Also

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

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)

VPR Score

3.6

EPSS Score

0.001

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: 2024/08/27

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 : libx11-6_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-6_2:1.6.4-3ubuntu0.4+esm1

  - Installed package : libx11-data_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-data_2:1.6.4-3ubuntu0.4+esm1

  - Installed package : libx11-xcb1_2:1.6.4-3ubuntu0.4
  - Fixed package     : libx11-xcb1_2:1.6.4-3ubuntu0.4+esm1
```

170185 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)

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-5813-1 advisory.

It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43945)

Tams Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42896)

It was discovered that the Xen netback driver in the Linux kernel did not properly handle packets structured in certain ways. An attacker in a guest VM could possibly use this to cause a denial of service (host NIC availability). (CVE-2022-3643)

It was discovered that an integer overflow vulnerability existed in the Bluetooth subsystem in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash).

(CVE-2022-45934)

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

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

See Also

https://ubuntu.com/security/notices/USN-5813-1

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)

VPR Score

6.7

EPSS Score

0.0016

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:5813-1

Plugin Information

Published: 2023/01/20, 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 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-137-generic
 for this advisory.
```

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)

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-1829
XREF	USN:6047-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-148-generic
 for this advisory.
```

200128 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GDK-PixBuf vulnerability (USN-6806-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6806-1 advisory.

Pedro Ribeiro and Vitor Pedreira discovered that the GDK-PixBuf library did not properly handle certain ANI files. An attacker could use this flaw to cause GDK-PixBuf to crash, resulting in a denial of service, or to possibly execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6806-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0008

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-2022-48622
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_2.36.11-2
  - Fixed package     : gir1.2-gdkpixbuf-2.0_2.36.11-2ubuntu0.1~esm1

  - Installed package : libgdk-pixbuf2.0-0_2.36.11-2
  - Fixed package     : libgdk-pixbuf2.0-0_2.36.11-2ubuntu0.1~esm1

  - Installed package : libgdk-pixbuf2.0-bin_2.36.11-2
  - Fixed package     : libgdk-pixbuf2.0-bin_2.36.11-2ubuntu0.1~esm1

  - Installed package : libgdk-pixbuf2.0-common_2.36.11-2
  - Fixed package     : libgdk-pixbuf2.0-common_2.36.11-2ubuntu0.1~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

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

CVSS v3.0 Temporal Score

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

VPR Score

4.7

EPSS Score

0.0004

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)

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	USN:6804-1

Plugin Information

Published: 2024/05/31, 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 : libc-bin_2.27-3ubuntu1.6
  - Fixed package     : libc-bin_2.27-3ubuntu1.6+esm3

  - Installed package : libc6_2.27-3ubuntu1.6
  - Fixed package     : libc6_2.27-3ubuntu1.6+esm3

  - Installed package : locales_2.27-3ubuntu1.6
  - Fixed package     : locales_2.27-3ubuntu1.6+esm3

  - Installed package : multiarch-support_2.27-3ubuntu1.6
  - Fixed package     : multiarch-support_2.27-3ubuntu1.6+esm3
```

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)

VPR Score

6.3

EPSS Score

0.0013

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_3.20230214.0ubuntu0.18.04.1
  - Fixed package     : intel-microcode_3.20240514.0ubuntu0.18.04.1+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0005

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_2.6-1
  - Fixed package     : python3-idna_2.6-1ubuntu0.1~esm1
```

193905 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6754-1 advisory.

It was discovered that nghttp2 incorrectly handled the HTTP/2 implementation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-9511, CVE-2019-9513)

It was discovered that nghttp2 incorrectly handled request cancellation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2023-44487)

It was discovered that nghttp2 could be made to process an unlimited number of HTTP/2 CONTINUATION frames.

A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. (CVE-2024-28182)

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

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

See Also

https://ubuntu.com/security/notices/USN-6754-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.8164

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-9511
CVE	CVE-2019-9513
CVE	CVE-2023-44487
CVE	CVE-2024-28182
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	USN:6754-1
XREF	CEA-ID:CEA-2024-0004
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2024/04/25, Modified: 2024/09/18

Plugin Output

tcp/0

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


  - Installed package : libnghttp2-14_1.30.0-1ubuntu1
  - Fixed package     : libnghttp2-14_1.30.0-1ubuntu1+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/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0004

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_3.20230214.0ubuntu0.18.04.1
  - Fixed package     : intel-microcode_3.20240813.0ubuntu0.18.04.1+esm2
```

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)

VPR Score

4.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-7006
XREF	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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm7
```

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)

VPR Score

4.4

EPSS Score

0.0011

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_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13+esm5

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13+esm5

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13+esm5
```

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.

Original advisory details:

Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner discovered

that Dnsmasq icorrectly handled validating DNSSEC messages. A remote

attacker could possibly use this issue to cause Dnsmasq to consume

resources, leading to a denial of service. (CVE-2023-50387)

It was discovered that Dnsmasq incorrectly handled preparing an NSEC3

closest encloser proof. A remote attacker could possibly use this issue to

cause Dnsmasq to consume resources, leading to a denial of service.

(CVE-2023-50868)

It was discovered that Dnsmasq incorrectly set the maximum EDNS.0 UDP

packet size as required by DNS Flag Day 2020. This issue only affected

Ubuntu 23.10. (CVE-2023-28450)

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

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

See Also

https://ubuntu.com/security/notices/USN-6657-2

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)

VPR Score

5.1

EPSS Score

0.05

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: 2024/08/28

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 : dnsmasq-base_2.79-1ubuntu0.7
  - Fixed package     : dnsmasq-base_2.90-0ubuntu0.18.04.1+esm1
```

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.

Original advisory details:

It was discovered that curl incorrectly handled memory when limiting the

amount of headers when HTTP/2 server push is allowed. A remote attacker

could possibly use this issue to cause curl to consume resources, leading

to a denial of service. (CVE-2024-2398)

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

Note that Nessus has not tested for 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

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

VPR Score

5.5

EPSS Score

0.0005

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-2024-2398
XREF	USN:6718-2
XREF	IAVA:2024-A-0185-S

Plugin Information

Published: 2024/03/27, 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 : libcurl3-gnutls_7.58.0-2ubuntu3.24
  - Fixed package     : libcurl3-gnutls_7.58.0-2ubuntu3.24+esm4
```

178653 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory.

Hangyu Hua discovered that the Flower classifier implementation in the Linux kernel contained an out-of-bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-35788, LP: #2023577)

It was discovered that for some Intel processors the INVLPG instruction implementation did not properly flush global TLB entries when PCIDs are enabled. An attacker could use this to expose sensitive information (kernel memory) or possibly cause undesired behaviors. (LP: #2023220)

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

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

See Also

https://ubuntu.com/security/notices/USN-6193-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-35788
XREF	USN:6193-1

Plugin Information

Published: 2023/07/20, Modified: 2024/09/19

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-153-generic
 for this advisory.
```

180004 - Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6302-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6302-1 advisory.

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2522, CVE-2022-2580, CVE-2022-2817, CVE-2022-2819, CVE-2022-2862, CVE-2022-2889, CVE-2022-2982, CVE-2022-3134)

It was discovered that Vim did not properly perform bounds checks in the diff mode in certain situations.

An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2598)

It was discovered that Vim did not properly perform bounds checks in certain situations. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS.

(CVE-2022-2816)

It was discovered that Vim incorrectly handled memory when skipping compiled code. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS.

(CVE-2022-2874)

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3016, CVE-2022-3037)

It was discovered that Vim incorrectly handled memory when invalid line number on :for is ignored. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3099)

It was discovered that Vim incorrectly handled memory when passing invalid arguments to the assert_fails() method. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3153)

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

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

See Also

https://ubuntu.com/security/notices/USN-6302-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0012

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-2522
CVE	CVE-2022-2580
CVE	CVE-2022-2598
CVE	CVE-2022-2816
CVE	CVE-2022-2817
CVE	CVE-2022-2819
CVE	CVE-2022-2862
CVE	CVE-2022-2874
CVE	CVE-2022-2889
CVE	CVE-2022-2982
CVE	CVE-2022-3016
CVE	CVE-2022-3037
CVE	CVE-2022-3099

CVE	CVE-2022-3134
CVE	CVE-2022-3153
XREF	IAVB:2022-B-0049-S
XREF	USN:6302-1

Plugin Information

Published: 2023/08/21, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm4

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm4

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm4
```

178914 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory.

It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3090)

Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges. (CVE-2023-32629)

It was discovered that the netfilter subsystem in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3390)

Tanguy Dubroca discovered that the netfilter subsystem in the Linux kernel did not properly handle certain pointer data type, leading to an out-of- bounds write vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35001)

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

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

See Also

https://ubuntu.com/security/notices/USN-6251-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2023-3090
CVE	CVE-2023-3390
CVE	CVE-2023-32629
CVE	CVE-2023-35001
XREF	USN:6251-1

Plugin Information

Published: 2023/07/26, 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.

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-155-generic
 for this advisory.
```

179937 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6301-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6301-1 advisory.

It was discovered that the netlink implementation in the Linux kernel did not properly validate policies when parsing attributes in some situations. An attacker could use this to cause a denial of service (infinite recursion). (CVE-2020-36691)

Billy Jheng Bing Jhong discovered that the CIFS network file system implementation in the Linux kernel did not properly validate arguments to ioctl() in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-0168)

It was discovered that the ext4 file system implementation in the Linux kernel contained a use-after-free vulnerability. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2022-1184)

It was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using a return address from a sibling thread. A local attacker could possibly use this to expose sensitive information. (CVE-2022-27672)

William Zhao discovered that the Traffic Control (TC) subsystem in the Linux kernel did not properly handle network packet retransmission in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-4269)

It was discovered that a race condition existed in the qdisc implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0590)

It was discovered that a race condition existed in the btrfs file system implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1611)

It was discovered that the APM X-Gene SoC hardware monitoring driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-1855)

It was discovered that the ST NCI NFC driver did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2023-1990)

It was discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation when mounting certain images. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service (system crash). (CVE-2023-2124)

It was discovered that the SLIMpro I2C device driver in the Linux kernel did not properly validate user-supplied data in some situations, leading to an out-of-bounds write vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-2194)

It was discovered that a race condition existed in the TLS subsystem in the Linux kernel, leading to a use-after-free or a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-28466)

It was discovered that the DA9150 charger driver in the Linux kernel did not properly handle device removal, leading to a user-after free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-30772)

It was discovered that the btrfs file system implementation in the Linux kernel did not properly handle error conditions in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-3111)

It was discovered that the Ricoh R5C592 MemoryStick card reader driver in the Linux kernel contained a race condition during module unload, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3141)

It was discovered that the Qualcomm EMAC ethernet driver in the Linux kernel did not properly handle device removal, leading to a user-after free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-33203)

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

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

See Also

https://ubuntu.com/security/notices/USN-6301-1

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)

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-36691
CVE	CVE-2022-0168
CVE	CVE-2022-1184
CVE	CVE-2022-4269
CVE	CVE-2022-27672
CVE	CVE-2023-0590
CVE	CVE-2023-1611
CVE	CVE-2023-1855
CVE	CVE-2023-1990
CVE	CVE-2023-2124
CVE	CVE-2023-2194
CVE	CVE-2023-3111
CVE	CVE-2023-3141
CVE	CVE-2023-28466
CVE	CVE-2023-30772
CVE	CVE-2023-33203
XREF	USN:6301-1

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.

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-156-generic
 for this advisory.
```

180257 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6317-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6317-1 advisory.

Daniel Moghimi discovered that some Intel(R) Processors did not properly clear microarchitectural state after speculative execution of various instructions. A local unprivileged user could use this to obtain to sensitive information. (CVE-2022-40982)

Tavis Ormandy discovered that some AMD processors did not properly handle speculative execution of certain vector register instructions. A local attacker could use this to expose sensitive information.

(CVE-2023-20593)

It was discovered that the universal 32bit network packet classifier implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3609)

It was discovered that the Quick Fair Queueing network scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3611)

It was discovered that the network packet classifier with netfilter/firewall marks implementation in the Linux kernel did not properly handle reference counting, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3776)

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

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

See Also

https://ubuntu.com/security/notices/USN-6317-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.1

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-40982
CVE	CVE-2023-3609
CVE	CVE-2023-3611
CVE	CVE-2023-3776
CVE	CVE-2023-20593
XREF	USN:6317-1

Plugin Information

Published: 2023/08/29, Modified: 2024/09/19

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-159-generic
 for this advisory.
```

180512 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6340-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6340-1 advisory.

Ruihan Li discovered that the bluetooth subsystem in the Linux kernel did not properly perform permissions checks when handling HCI sockets. A physically proximate attacker could use this to cause a denial of service (bluetooth communication). (CVE-2023-2002)

Zi Fan Tan discovered that the binder IPC implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-21255)

Juan Jose Lopez Jaimez, Meador Inge, Simon Scannell, and Nenad Stojanovski discovered that the BPF verifier in the Linux kernel did not properly mark registers for precision tracking in certain situations, leading to an out- of-bounds access vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-2163)

Zheng Zhang discovered that the device-mapper implementation in the Linux kernel did not properly handle locking during table_clear() operations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2269)

It was discovered that the DVB Core driver in the Linux kernel did not properly handle locking events in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock).

(CVE-2023-31084)

It was discovered that the kernel->user space relay implementation in the Linux kernel did not properly perform certain buffer calculations, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-3268)

It was discovered that the video4linux driver for Philips based TV cards in the Linux kernel contained a race condition during device removal, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-35823)

It was discovered that the SDMC DM1105 PCI device driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35824)

It was discovered that the Renesas USB controller driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35828)

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

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

See Also

https://ubuntu.com/security/notices/USN-6340-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/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:H/I:H/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-2002
CVE	CVE-2023-2163
CVE	CVE-2023-2269
CVE	CVE-2023-3268
CVE	CVE-2023-21255
CVE	CVE-2023-31084

CVE	CVE-2023-35823
CVE	CVE-2023-35824
CVE	CVE-2023-35828
XREF	USN:6340-1

Plugin Information

Published: 2023/09/05, Modified: 2024/09/18

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-162-generic
 for this advisory.
```

181641 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6387-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6387-1 advisory.

Jana Hofmann, Emanuele Vannacci, Cedric Fournet, Boris Kopf, and Oleksii Oleksenko discovered that some AMD processors could leak stale data from division operations in certain situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-20588)

It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle L2CAP socket release, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-40283)

It was discovered that some network classifier implementations in the Linux kernel contained use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4128)

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

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

See Also

https://ubuntu.com/security/notices/USN-6387-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2023-4128
CVE	CVE-2023-20588
CVE	CVE-2023-40283
XREF	USN:6387-1

Plugin Information

Published: 2023/09/19, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-163-generic
 for this advisory.
```

183455 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6441-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6441-1 advisory.

Ross Lagerwall discovered that the Xen netback backend driver in the Linux kernel did not properly handle certain unusual packets from a paravirtualized network frontend, leading to a buffer overflow. An attacker in a guest VM could use this to cause a denial of service (host system crash) or possibly execute arbitrary code. (CVE-2023-34319)

Kyle Zeng discovered that the networking stack implementation in the Linux kernel did not properly validate skb object size in certain conditions. An attacker could use this cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42752)

Kyle Zeng discovered that the netfiler subsystem in the Linux kernel did not properly calculate array offsets, leading to a out-of-bounds write vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42753)

Kyle Zeng discovered that the IPv4 Resource Reservation Protocol (RSVP) classifier implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash). Please note that kernel packet classifier support for RSVP has been removed to resolve this vulnerability. (CVE-2023-42755)

Kyle Zeng discovered that the netfilter subsystem in the Linux kernel contained a race condition in IP set operations in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-42756)

Bing-Jhong Billy Jheng discovered that the Unix domain socket implementation in the Linux kernel contained a race condition in certain situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4622)

Budimir Markovic discovered that the qdisc implementation in the Linux kernel did not properly validate inner classes, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4623)

Alex Birnberg discovered that the netfilter subsystem in the Linux kernel did not properly validate register length, leading to an out-of- bounds write vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-4881)

It was discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel did not properly handle network packets in certain conditions, leading to a use after free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-4921)

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

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

See Also

https://ubuntu.com/security/notices/USN-6441-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2023-4622
CVE	CVE-2023-4623
CVE	CVE-2023-4881
CVE	CVE-2023-4921
CVE	CVE-2023-34319
CVE	CVE-2023-42752
CVE	CVE-2023-42753
CVE	CVE-2023-42755
CVE	CVE-2023-42756
XREF	USN:6441-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-165-generic
 for this advisory.
```

186082 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6495-1 advisory.

Yu Hao discovered that the UBI driver in the Linux kernel did not properly check for MTD with zero erasesize during device attachment. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-31085)

Manfred Rudigier discovered that the Intel(R) PCI-Express Gigabit (igb) Ethernet driver in the Linux kernel did not properly validate received frames that are larger than the set MTU size, leading to a buffer overflow vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-45871)

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

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

See Also

https://ubuntu.com/security/notices/USN-6495-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-31085
CVE	CVE-2023-45871
XREF	USN:6495-1

Plugin Information

Published: 2023/11/21, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-167-generic
 for this advisory.
```

186743 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6548-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6548-1 advisory.

It was discovered that Spectre-BHB mitigations were missing for Ampere processors. A local attacker could potentially use this to expose sensitive information. (CVE-2023-3006)

It was discovered that the USB subsystem in the Linux kernel contained a race condition while handling device descriptors in certain situations, leading to a out-of-bounds read vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-37453)

Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate some attributes passed from userspace. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2023-39189)

Sunjoo Park discovered that the netfilter subsystem in the Linux kernel did not properly validate u32 packets content, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39192)

Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate SCTP data, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39193)

Lucas Leong discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel did not properly handle state filters, leading to an out- of-bounds read vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39194)

Kyle Zeng discovered that the IPv4 implementation in the Linux kernel did not properly handle socket buffers (skb) when performing IP routing in certain circumstances, leading to a null pointer dereference vulnerability. A privileged attacker could use this to cause a denial of service (system crash).

(CVE-2023-42754)

Alon Zahavi discovered that the NVMe-oF/TCP subsystem in the Linux kernel did not properly handle queue initialization failures in certain situations, leading to a use-after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-5178)

Budimir Markovic discovered that the perf subsystem in the Linux kernel did not properly handle event groups, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-5717)

It was discovered that the TLS subsystem in the Linux kernel did not properly perform cryptographic operations in some situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6176)

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

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

See Also

https://ubuntu.com/security/notices/USN-6548-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0243

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-3006
CVE	CVE-2023-5178
CVE	CVE-2023-5717
CVE	CVE-2023-6176
CVE	CVE-2023-37453
CVE	CVE-2023-39189
CVE	CVE-2023-39192

CVE	CVE-2023-39193
CVE	CVE-2023-39194
CVE	CVE-2023-42754
XREF	USN:6548-1

Plugin Information

Published: 2023/12/11, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-169-generic
 for this advisory.
```

189614 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6605-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6605-1 advisory.

Lin Ma discovered that the netfilter subsystem in the Linux kernel did not properly validate network family support while creating a new netfilter table. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6040)

It was discovered that the CIFS network file system implementation in the Linux kernel did not properly validate the server frame size in certain situation, leading to an out-of-bounds read vulnerability. An attacker could use this to construct a malicious CIFS image that, when operated on, could cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-6606)

Budimir Markovic, Lucas De Marchi, and Pengfei Xu discovered that the perf subsystem in the Linux kernel did not properly validate all event sizes when attaching new events, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6931)

It was discovered that the IGMP protocol implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6932)

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

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

See Also

https://ubuntu.com/security/notices/USN-6605-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-6040
CVE	CVE-2023-6606
CVE	CVE-2023-6931
CVE	CVE-2023-6932
XREF	USN:6605-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-170-generic
 for this advisory.
```

190124 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6625-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6625-1 advisory.

Marek Marczykowski-Grecki discovered that the Xen event channel infrastructure implementation in the Linux kernel contained a race condition. An attacker in a guest VM could possibly use this to cause a denial of service (paravirtualized device unavailability). (CVE-2023-34324)

Zheng Wang discovered a use-after-free in the Renesas Ethernet AVB driver in the Linux kernel during device removal. A privileged attacker could use this to cause a denial of service (system crash).

(CVE-2023-35827)

It was discovered that a race condition existed in the Linux kernel when performing operations with kernel objects, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2023-45863)

discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel did not properly handle certain memory allocation failure conditions, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2023-46343)

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

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

See Also

https://ubuntu.com/security/notices/USN-6625-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

6.0 (CVSS2#AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-34324
CVE	CVE-2023-35827
CVE	CVE-2023-45863
CVE	CVE-2023-46343
XREF	USN:6625-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-171-generic
 for this advisory.
```

183751 - Ubuntu 18.04 ESM : libvpx vulnerabilities (USN-6403-2)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6403-2 advisory.

USN-6403-1 fixed several vulnerabilities in libvpx. This update provides the corresponding update for Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that libvpx did not properly handle certain malformed

media files. If an application using libvpx opened a specially crafted

file, a remote attacker could cause a denial of service, or possibly

execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6403-2

Solution

Update the affected libvpx-dev, libvpx5 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)

VPR Score

7.4

EPSS Score

0.3061

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5217
CVE	CVE-2023-44488
XREF	CISA-KNOWN-EXPLOITED:2023/10/23
XREF	USN:6403-2

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 : libvpx5_1.7.0-3ubuntu0.18.04.1
  - Fixed package     : libvpx5_1.7.0-3ubuntu0.18.04.1+esm1
```

182081 - Ubuntu 18.04 ESM : libwebp vulnerability (USN-6369-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6369-2 advisory.

USN-6369-1 fixed a vulnerability in libwebp. This update provides the corresponding update for Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that libwebp incorrectly handled certain malformed

images.

If a user or automated system were tricked into opening a

specially crafted image file, a remote attacker could use this issue to

cause libwebp to crash, resulting in a denial of service, or possibly

execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6369-2

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

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

VPR Score

9.8

EPSS Score

0.6295

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-4863
XREF	CISA-KNOWN-EXPLOITED:2023/10/04
XREF	USN:6369-2

Plugin Information

Published: 2023/09/28, 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 : libwebp6_0.6.1-2ubuntu0.18.04.2
  - Fixed package     : libwebp6_0.6.1-2ubuntu0.18.04.2+esm1

  - Installed package : libwebpdemux2_0.6.1-2ubuntu0.18.04.2
  - Fixed package     : libwebpdemux2_0.6.1-2ubuntu0.18.04.2+esm1

  - Installed package : libwebpmux3_0.6.1-2ubuntu0.18.04.2
  - Fixed package     : libwebpmux3_0.6.1-2ubuntu0.18.04.2+esm1
```

191499 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : python-cryptography vulnerabilities (USN-6673-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6673-1 advisory.

Hubert Kario discovered that python-cryptography incorrectly handled

errors returned by the OpenSSL API when processing incorrect padding in

RSA PKCS#1 v1.5. A remote attacker could possibly use this issue to expose

confidential or sensitive information. (CVE-2023-50782)

It was discovered that python-cryptography incorrectly handled memory

operations when processing mismatched PKCS#12 keys. A remote attacker could

possibly use this issue to cause python-cryptography to crash, leading to a denial of service. This issue only affected Ubuntu 23.10. (CVE-2024-26130)

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

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

See Also

https://ubuntu.com/security/notices/USN-6673-1

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-50782
CVE	CVE-2024-26130
XREF	USN:6673-1

Plugin Information

Published: 2024/03/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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_2.1.4-1ubuntu1.4
  - Fixed package     : python3-cryptography_2.1.4-1ubuntu1.4+esm1
```

153769 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5091-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5091-1 advisory.

Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack.

An attacker could use this to expose sensitive information. (CVE-2021-33624)

It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. (CVE-2021-3679)

Alexey Kardashevskiy discovered that the KVM implementation for PowerPC systems in the Linux kernel did not properly validate RTAS arguments in some situations. An attacker in a guest vm could use this to cause a denial of service (host OS crash) or possibly execute arbitrary code. (CVE-2021-37576)

It was discovered that the Virtio console implementation in the Linux kernel did not properly validate input lengths in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-38160)

Michael Wakabayashi discovered that the NFSv4 client implementation in the Linux kernel did not properly order connection setup operations. An attacker controlling a remote NFS server could use this to cause a denial of service on the client. (CVE-2021-38199)

It was discovered that the MAX-3421 host USB device driver in the Linux kernel did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-38204)

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

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

See Also

https://ubuntu.com/security/notices/USN-5091-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3679
CVE	CVE-2021-33624
CVE	CVE-2021-37576
CVE	CVE-2021-38160
CVE	CVE-2021-38199
CVE	CVE-2021-38204
XREF	USN:5091-1

Plugin Information

Published: 2021/09/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-87-generic
 for this advisory.
```

154278 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5116-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5116-1 advisory.

It was discovered that a race condition existed in the Atheros Ath9k WiFi driver in the Linux kernel. An attacker could possibly use this to expose sensitive information (WiFi network traffic). (CVE-2020-3702)

Alois Wohlschlager discovered that the overlay file system in the Linux kernel did not restrict private clones in some situations. An attacker could use this to expose sensitive information. (CVE-2021-3732)

It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly compute the access permissions for shadow pages in some situations. A local attacker could use this to cause a denial of service. (CVE-2021-38198)

It was discovered that the Xilinx 10/100 Ethernet Lite device driver in the Linux kernel could report pointer addresses in some situations. An attacker could use this information to ease the exploitation of another vulnerability. (CVE-2021-38205)

It was discovered that the ext4 file system in the Linux kernel contained a race condition when writing 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-5116-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.001

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-2021-3732
CVE	CVE-2021-38198
CVE	CVE-2021-38205
CVE	CVE-2021-40490
CVE	CVE-2021-42008
XREF	USN:5116-1

Plugin Information

Published: 2021/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-89-generic
 for this advisory.
```

154980 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5137-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5137-1 advisory.

It was discovered that the f2fs file system in the Linux kernel did not properly validate metadata in some situations. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-19449)

It was discovered that the Infiniband RDMA userspace connection manager implementation in the Linux kernel contained a race condition leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possible execute arbitrary code. (CVE-2020-36385)

Wolfgang Frisch discovered that the ext4 file system implementation in the Linux kernel contained an integer overflow when handling metadata inode extents. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2021-3428)

Benedict Schlueter discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side- channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-34556)

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side-channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-35477)

It was discovered that the btrfs file system in the Linux kernel did not properly handle removing a non-existent device id. An attacker with CAP_SYS_ADMIN could use this to cause a denial of service.

(CVE-2021-3739)

It was discovered that the Qualcomm IPC Router protocol implementation in the Linux kernel did not properly validate metadata in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2021-3743)

It was discovered that the virtual terminal (vt) device implementation in the Linux kernel contained a race condition in its ioctl handling that led to an out-of-bounds read vulnerability. A local attacker could possibly use this to expose sensitive information. (CVE-2021-3753)

It was discovered that the Linux kernel did not properly account for the memory usage of certain IPC objects. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3759)

It was discovered that the Aspeed Low Pin Count (LPC) Bus Controller implementation in the Linux kernel did not properly perform boundary checks in some situations, allowing out-of-bounds write access. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. In Ubuntu, this issue only affected systems running armhf kernels. (CVE-2021-42252)

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

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

See Also

https://ubuntu.com/security/notices/USN-5137-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0013

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-19449
CVE	CVE-2020-36385
CVE	CVE-2021-3428
CVE	CVE-2021-3739
CVE	CVE-2021-3743
CVE	CVE-2021-3753
CVE	CVE-2021-3759
CVE	CVE-2021-34556
CVE	CVE-2021-35477
CVE	CVE-2021-42252

XREF USN:5137-1

Plugin Information

Published: 2021/11/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-90-generic
 for this advisory.
```

156481 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5210-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5210-1 advisory.

Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. (CVE-2021-4002)

It was discovered that the Linux kernel did not properly enforce certain types of entries in the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. An attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2020-26541)

It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-20321)

It was discovered that the NFC subsystem in the Linux kernel contained a use-after-free vulnerability in its NFC Controller Interface (NCI) implementation. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-3760)

It was discovered that an integer overflow could be triggered in the eBPF implementation in the Linux kernel when preallocating objects for stack maps. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-41864)

It was discovered that the KVM implementation for POWER8 processors in the Linux kernel did not properly keep track if a wakeup event could be resolved by a guest. An attacker in a guest VM could possibly use this to cause a denial of service (host OS crash). (CVE-2021-43056)

It was discovered that the ISDN CAPI implementation in the Linux kernel contained a race condition in certain situations that could trigger an array out-of-bounds bug. A privileged local attacker could possibly use this to cause a denial of service or execute arbitrary code. (CVE-2021-43389)

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

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

See Also

https://ubuntu.com/security/notices/USN-5210-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-26541
CVE	CVE-2021-3760
CVE	CVE-2021-4002
CVE	CVE-2021-20321
CVE	CVE-2021-41864
CVE	CVE-2021-43056
CVE	CVE-2021-43389
XREF	USN:5210-1

Plugin Information

Published: 2022/01/06, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-92-generic
 for this advisory.
```

157353 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5267-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5267-1 advisory.

It was discovered that the Bluetooth subsystem in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3640)

Likang Luo discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-3752)

Luo Likang discovered that the FireDTV Firewire driver in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-42739)

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

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

See Also

https://ubuntu.com/security/notices/USN-5267-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0012

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3640
CVE	CVE-2021-3752
CVE	CVE-2021-42739
XREF	USN:5267-1

Plugin Information

Published: 2022/02/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-97-generic
 for this advisory.
```

158253 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5294-2)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5294-2 advisory.

It was discovered that the Packet network protocol implementation in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-22600)

Szymon Heidrich discovered that the USB Gadget subsystem in the Linux kernel did not properly restrict the size of control requests for certain gadget types, leading to possible out of bounds reads or writes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-39685)

Jann Horn discovered a race condition in the Unix domain socket implementation in the Linux kernel that could result in a read-after-free. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-4083)

Kirill Tkhai discovered that the XFS file system implementation in the Linux kernel did not calculate size correctly when pre-allocating space in some situations. A local attacker could use this to expose sensitive information. (CVE-2021-4155)

Lin Ma discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-4202)

Brendan Dolan-Gavitt discovered that the aQuantia AQtion Ethernet device driver in the Linux kernel did not properly validate meta-data coming from the device. A local attacker who can control an emulated device can use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2021-43975)

Sushma Venkatesh Reddy discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-0330)

It was discovered that the VMware Virtual GPU driver in the Linux kernel did not properly handle certain failure conditions, leading to a stale entry in the file descriptor table. A local attacker could use this to expose sensitive information or possibly gain administrative privileges. (CVE-2022-22942)

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

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

See Also

https://ubuntu.com/security/notices/USN-5294-2

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)

VPR Score

9.2

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-4083
CVE	CVE-2021-4155
CVE	CVE-2021-4202
CVE	CVE-2021-22600
CVE	CVE-2021-39685
CVE	CVE-2021-43975
CVE	CVE-2022-0330
CVE	CVE-2022-22942
XREF	USN:5294-2
XREF	CISA-KNOWN-EXPLOITED:2022/05/02

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/02/22, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-100-generic
 for this advisory.
```

158737 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5318-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5318-1 advisory.

Nick Gregory discovered that the Linux kernel incorrectly handled network offload functionality. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-25636)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by ARM to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-23960)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by Intel to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-0001, CVE-2022-0002)

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

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

See Also

https://ubuntu.com/security/notices/USN-5318-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.0

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0001
CVE	CVE-2022-0002
CVE	CVE-2022-23960
CVE	CVE-2022-25636
XREF	USN:5318-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2022/03/09, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-104-generic
 for this advisory.
```

159144 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5338-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5338-1 advisory.

Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. (CVE-2022-0492)

Jrgen Gro discovered that the Xen subsystem within the Linux kernel did not adequately limit the number of events driver domains (unprivileged PV backends) could send to other guest VMs. An attacker in a driver domain could use this to cause a denial of service in other guest VMs. (CVE-2021-28711, CVE-2021-28712, CVE-2021-28713)

Jrgen Gro discovered that the Xen network backend driver in the Linux kernel did not adequately limit the amount of queued packets when a guest did not process them. An attacker in a guest VM can use this to cause a denial of service (excessive kernel memory consumption) in the network backend domain.

(CVE-2021-28714, CVE-2021-28715)

It was discovered that the simulated networking device driver for the Linux kernel did not properly initialize memory in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-4135)

Brendan Dolan-Gavitt discovered that the Marvell WiFi-Ex USB device driver in the Linux kernel did not properly handle some error conditions. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-43976)

It was discovered that the ARM Trusted Execution Environment (TEE) subsystem in the Linux kernel contained a race condition leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-44733)

It was discovered that the Phone Network protocol (PhoNet) implementation in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45095)

It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45480)

Samuel Page discovered that the Transparent Inter-Process Communication (TIPC) protocol implementation in the Linux kernel contained a stack-based buffer overflow. A remote attacker could use this to cause a denial of service (system crash) for systems that have a TIPC bearer configured. (CVE-2022-0435)

It was discovered that the KVM implementation for s390 systems in the Linux kernel did not properly prevent memory operations on PVM guests that were in non-protected mode. A local attacker could use this to obtain unauthorized memory write access. (CVE-2022-0516)

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

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

See Also

https://ubuntu.com/security/notices/USN-5338-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.0951

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-4135
CVE	CVE-2021-28711
CVE	CVE-2021-28712
CVE	CVE-2021-28713
CVE	CVE-2021-28714
CVE	CVE-2021-28715
CVE	CVE-2021-43976

CVE	CVE-2021-44733
CVE	CVE-2021-45095
CVE	CVE-2021-45480
CVE	CVE-2022-0435
CVE	CVE-2022-0492
CVE	CVE-2022-0516
XREF	USN:5338-1

Exploitable With

Metasploit (true)

Plugin Information

Published: 2022/03/22, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-105-generic
 for this advisory.
```

159373 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5358-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5358-1 advisory.

It was discovered that the network traffic control implementation in the Linux kernel contained a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1055)

It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2022-27666)

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

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

See Also

https://ubuntu.com/security/notices/USN-5358-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-1055
CVE	CVE-2022-27666
XREF	USN:5358-1

Exploitable With

CANVAS (true)

Plugin Information

Published: 2022/03/31, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-107-generic
 for this advisory.
```

161063 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5415-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5415-1 advisory.

Jeremy Cline discovered a use-after-free in the nouveau graphics driver of the Linux kernel during device removal. A privileged or physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-27820)

Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information.

(CVE-2021-26401)

David Bouman discovered that the netfilter subsystem in the Linux kernel did not initialize memory in some situations. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2022-1016)

It was discovered that the MMC/SD subsystem in the Linux kernel did not properly handle read errors from SD cards in certain situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-20008)

It was discovered that the USB gadget subsystem in the Linux kernel did not properly validate interface descriptor requests. An attacker could possibly use this to cause a denial of service (system crash).

(CVE-2022-25258)

It was discovered that the Remote NDIS (RNDIS) USB gadget implementation in the Linux kernel did not properly validate the size of the RNDIS_MSG_SET command. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-25375)

It was discovered that the ST21NFCA NFC driver in the Linux kernel did not properly validate the size of certain data in EVT_TRANSACTION events. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-26490)

It was discovered that the Xilinx USB2 device gadget driver in the Linux kernel did not properly validate endpoint indices from the host. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-27223)

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

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

See Also

https://ubuntu.com/security/notices/USN-5415-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-27820
CVE	CVE-2021-26401
CVE	CVE-2022-1016
CVE	CVE-2022-20008
CVE	CVE-2022-25258
CVE	CVE-2022-25375
CVE	CVE-2022-26490
CVE	CVE-2022-27223
XREF	USN:5415-1

Plugin Information

Published: 2022/05/12, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-110-generic
 for this advisory.
```

161810 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5442-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5442-1 advisory.

Kyle Zeng discovered that the Network Queuing and Scheduling subsystem of the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

(CVE-2022-29581)

Bing-Jhong Billy Jheng discovered that the io_uring subsystem in the Linux kernel contained in integer overflow. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1116)

Jann Horn discovered that the Linux kernel did not properly enforce seccomp restrictions in some situations. A local attacker could use this to bypass intended seccomp sandbox restrictions.

(CVE-2022-30594)

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

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

See Also

https://ubuntu.com/security/notices/USN-5442-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-1116
CVE	CVE-2022-29581
CVE	CVE-2022-30594
XREF	USN:5442-1

Plugin Information

Published: 2022/06/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-113-generic
 for this advisory.
```

161950 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5467-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5467-1 advisory.

It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2022-21499)

Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

(CVE-2022-1966)

It was discovered that the SCTP protocol implementation in the Linux kernel did not properly verify VTAGs in some situations. A remote attacker could possibly use this to cause a denial of service (connection disassociation). (CVE-2021-3772)

Eric Biederman discovered that the cgroup process migration implementation in the Linux kernel did not perform permission checks correctly in some situations. A local attacker could possibly use this to gain administrative privileges. (CVE-2021-4197)

Jann Horn discovered that the FUSE file system in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1011)

Qiuhao Li, Gaoning Pan and Yongkang Jia discovered that the KVM implementation in the Linux kernel did not properly perform guest page table updates in some situations. An attacker in a guest vm could possibly use this to crash the host OS. (CVE-2022-1158)

Duoming Zhou discovered that the 6pack protocol implementation in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-1198)

It was discovered that the PF_KEYv2 implementation in the Linux kernel did not properly initialize kernel memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-1353)

It was discovered that the implementation of X.25 network protocols in the Linux kernel did not terminate link layer sessions properly. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1516)

Demi Marie Obenour and Simon Gaiser discovered that several Xen para- virtualization device frontends did not properly restrict the access rights of device backends. An attacker could possibly use a malicious Xen backend to gain access to memory pages of a guest VM or cause a denial of service in the guest.

(CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042)

It was discovered that the USB Gadget file system interface in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-24958)

It was discovered that the USB SR9700 ethernet device driver for the Linux kernel did not properly validate the length of requests from the device. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-26966)

discovered that the 802.2 LLC type 2 driver in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could use this to cause a denial of service.

(CVE-2022-28356)

It was discovered that the Microchip CAN BUS Analyzer interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-28389)

It was discovered that the EMS CAN/USB interface implementation in the Linux kernel contained a double-free vulnerability when handling certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-28390)

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

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

See Also

https://ubuntu.com/security/notices/USN-5467-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0052

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3772
CVE	CVE-2021-4197
CVE	CVE-2022-1011
CVE	CVE-2022-1158
CVE	CVE-2022-1198
CVE	CVE-2022-1353
CVE	CVE-2022-1516
CVE	CVE-2022-21499
CVE	CVE-2022-23036
CVE	CVE-2022-23037
CVE	CVE-2022-23038
CVE	CVE-2022-23039
CVE	CVE-2022-23040
CVE	CVE-2022-23041
CVE	CVE-2022-23042
CVE	CVE-2022-24958
CVE	CVE-2022-26966
CVE	CVE-2022-28356
CVE	CVE-2022-28389
CVE	CVE-2022-28390
XREF	USN:5467-1

Plugin Information

Published: 2022/06/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-117-generic
 for this advisory.
```

164036 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5562-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5562-1 advisory.

Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2588)

It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2586)

It was discovered that the block layer subsystem in the Linux kernel did not properly initialize memory in some situations. A privileged local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-0494)

Hu Jiahui discovered that multiple race conditions existed in the Advanced Linux Sound Architecture (ALSA) framework, leading to use-after-free vulnerabilities. A local attacker could use these to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1048)

Minh Yuan discovered that the floppy disk driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1652)

It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1679)

It was discovered that the Marvell NFC device driver implementation in the Linux kernel did not properly perform memory cleanup operations in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code.

(CVE-2022-1734)

Duoming Zhou discovered a race condition in the NFC subsystem in the Linux kernel, leading to a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1974)

Duoming Zhou discovered that the NFC subsystem in the Linux kernel did not properly prevent context switches from occurring during certain atomic context operations. A privileged local attacker could use this to cause a denial of service (system crash). (CVE-2022-1975)

Felix Fu discovered that the Sun RPC implementation in the Linux kernel did not properly handle socket states, leading to a use-after-free vulnerability. A remote attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-28893)

Arthur Mongodin discovered that the netfilter subsystem in the Linux kernel did not properly perform data validation. A local attacker could use this to escalate privileges in certain situations. (CVE-2022-34918)

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

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

See Also

https://ubuntu.com/security/notices/USN-5562-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.7

EPSS Score

0.0068

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0494
CVE	CVE-2022-1048
CVE	CVE-2022-1652
CVE	CVE-2022-1679
CVE	CVE-2022-1734
CVE	CVE-2022-1974
CVE	CVE-2022-1975

CVE	CVE-2022-2586
CVE	CVE-2022-2588
CVE	CVE-2022-28893
CVE	CVE-2022-34918
XREF	USN:5562-1
XREF	CISA-KNOWN-EXPLOITED:2024/07/17

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

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

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-124-generic
 for this advisory.
```

165287 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5622-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5622-1 advisory.

It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of- bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33655)

Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information. (CVE-2022-1012, CVE-2022-32296)

Norbert Slusarek discovered that a race condition existed in the perf subsystem in the Linux kernel, resulting in a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1729)

It was discovered that the device-mapper verity (dm-verity) driver in the Linux kernel did not properly verify targets being loaded into the device- mapper table. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2503)

Domingo Dirutigliano and Nicola Guerrera discovered that the netfilter subsystem in the Linux kernel did not properly handle rules that truncated packets below the packet header size. When such rules are in place, a remote attacker could possibly use this to cause a denial of service (system crash).

(CVE-2022-36946)

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

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

See Also

https://ubuntu.com/security/notices/USN-5622-1

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-33655
CVE	CVE-2022-1012
CVE	CVE-2022-1729
CVE	CVE-2022-2503
CVE	CVE-2022-32296
CVE	CVE-2022-36946
XREF	USN:5622-1

Plugin Information

Published: 2022/09/21, Modified: 2024/08/29

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-126-generic
 for this advisory.
```

166012 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5668-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5668-1 advisory.

It was discovered that the BPF verifier in the Linux kernel did not properly handle internal data structures. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2021-4159)

It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 (V4L2) implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-20369)

Duoming Zhou discovered that race conditions existed in the timer handling implementation of the Linux kernel's Rose X.25 protocol layer, resulting in use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-2318)

Roger Pau Monn discovered that the Xen virtual block driver in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-26365)

Pawan Kumar Gupta, Alyssa Milburn, Amit Peled, Shani Rehana, Nir Shildan and Ariel Sabba discovered that some Intel processors with Enhanced Indirect Branch Restricted Speculation (eIBRS) did not properly handle RET instructions after a VM exits. A local attacker could potentially use this to expose sensitive information. (CVE-2022-26373)

Eric Biggers discovered that a use-after-free vulnerability existed in the io_uring subsystem in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3176)

Roger Pau Monn discovered that the Xen paravirtualization frontend in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-33740)

It was discovered that the Xen paravirtualization frontend in the Linux kernel incorrectly shared unrelated data when communicating with certain backends. A local attacker could use this to cause a denial of service (guest crash) or expose sensitive information (guest kernel memory). (CVE-2022-33741, CVE-2022-33742)

Oleksandr Tyshchenko discovered that the Xen paravirtualization platform in the Linux kernel on ARM platforms contained a race condition in certain situations. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2022-33744)

It was discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a reference counting error. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-36879)

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

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

See Also

https://ubuntu.com/security/notices/USN-5668-1

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-4159
CVE	CVE-2022-2318
CVE	CVE-2022-3176
CVE	CVE-2022-20369
CVE	CVE-2022-26365
CVE	CVE-2022-26373
CVE	CVE-2022-33740

CVE	CVE-2022-33741
CVE	CVE-2022-33742
CVE	CVE-2022-33744
CVE	CVE-2022-36879
XREF	USN:5668-1

Plugin Information

Published: 2022/10/11, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-128-generic
 for this advisory.
```

166286 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5691-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5691-1 advisory.

David Bouman and Billy Jheng Bing Jhong discovered that a race condition existed in the io_uring subsystem in the Linux kernel, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2602)

Snke Huster discovered that an integer overflow vulnerability existed in the WiFi driver stack in the Linux kernel, leading to a buffer overflow. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41674)

Snke Huster discovered that the WiFi driver stack in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2022-42720)

Snke Huster discovered that the WiFi driver stack in the Linux kernel did not properly handle BSSID/SSID lists in some situations. A physically proximate attacker could use this to cause a denial of service (infinite loop). (CVE-2022-42721)

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

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

See Also

https://ubuntu.com/security/notices/USN-5691-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0019

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2602
CVE	CVE-2022-41674
CVE	CVE-2022-42720
CVE	CVE-2022-42721
XREF	USN:5691-1

Plugin Information

Published: 2022/10/20, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-131-generic
 for this advisory.
```

167771 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5728-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5728-1 advisory.

Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)

It was discovered that a race condition existed in the memory address space accounting implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41222)

It was discovered that a race condition existed in the instruction emulator of the Linux kernel on Arm 64-bit systems. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-20422)

It was discovered that the KVM implementation in the Linux kernel did not properly handle virtual CPUs without APICs in certain situations. A local attacker could possibly use this to cause a denial of service (host system crash). (CVE-2022-2153)

Hao Sun and Jiacheng Xu discovered that the NILFS file system implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2978)

Johannes Wikner and Kaveh Razavi discovered that for some Intel x86-64 processors, the Linux kernel's protections against speculative branch target injection attacks were insufficient in some circumstances. A local attacker could possibly use this to expose sensitive information. (CVE-2022-29901)

Abhishek Shah discovered a race condition in the PF_KEYv2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3028)

It was discovered that the Netlink device interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability with some network device drivers. A local attacker with admin access to the network device could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3625)

It was discovered that the IDT 77252 ATM PCI device driver in the Linux kernel did not properly remove any pending timers during device exit, resulting in a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-3635)

Xingyuan Mo and Gengjia Chen discovered that the Promise SuperTrak EX storage controller driver in the Linux kernel did not properly handle certain structures. A local attacker could potentially use this to expose sensitive information (kernel memory). (CVE-2022-40768)

Snke Huster discovered that a use-after-free vulnerability existed in the WiFi driver stack in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42719)

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

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

See Also

https://ubuntu.com/security/notices/USN-5728-1

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0099

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2153
CVE	CVE-2022-2978
CVE	CVE-2022-3028
CVE	CVE-2022-3625
CVE	CVE-2022-3635
CVE	CVE-2022-20422

CVE	CVE-2022-29901
CVE	CVE-2022-40768
CVE	CVE-2022-41222
CVE	CVE-2022-42703
CVE	CVE-2022-42719
XREF	USN:5728-1

Plugin Information

Published: 2022/11/17, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-132-generic
 for this advisory.
```

168348 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5756-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5756-1 advisory.

Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)

It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3524)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3564)

It was discovered that the ISDN implementation of the Linux kernel contained a use-after-free vulnerability. A privileged user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3565)

It was discovered that the TCP implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3566)

It was discovered that the IPv6 implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3567)

It was discovered that the Realtek RTL8152 USB Ethernet adapter driver in the Linux kernel did not properly handle certain error conditions. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3594)

It was discovered that a null pointer dereference existed in the NILFS2 file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3621)

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

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

See Also

https://ubuntu.com/security/notices/USN-5756-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-3524
CVE	CVE-2022-3564
CVE	CVE-2022-3565
CVE	CVE-2022-3566
CVE	CVE-2022-3567
CVE	CVE-2022-3594
CVE	CVE-2022-3621
CVE	CVE-2022-42703
XREF	USN:5756-1

Plugin Information

Published: 2022/12/02, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-135-generic
 for this advisory.
```

169689 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory.

It was discovered that a race condition existed in the Android Binder IPC subsystem in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-20421)

David Leadbeater discovered that the netfilter IRC protocol tracking implementation in the Linux Kernel incorrectly handled certain message payloads in some situations. A remote attacker could possibly use this to cause a denial of service or bypass firewall filtering. (CVE-2022-2663)

It was discovered that the Intel 740 frame buffer driver in the Linux kernel contained a divide by zero vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-3061)

It was discovered that the sound subsystem in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3303)

Gwnaun Jung discovered that the SFB packet scheduling implementation in the Linux kernel contained a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3586)

It was discovered that the NILFS2 file system implementation in the Linux kernel did not properly deallocate memory in certain error conditions. An attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3646)

Hyunwoo Kim discovered that an integer overflow vulnerability existed in the PXA3xx graphics driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash).

(CVE-2022-39842)

It was discovered that a race condition existed in the EFI capsule loader driver in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-40307)

Zheng Wang and Zhuorao Yang discovered that the RealTek RTL8712U wireless driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-4095)

It was discovered that the USB monitoring (usbmon) component in the Linux kernel did not properly set permissions on memory mapped in to user space processes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43750)

Jann Horn discovered a race condition existed in the Linux kernel when unmapping VMAs in certain situations, resulting in possible use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-39188)

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

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

See Also

https://ubuntu.com/security/notices/USN-5791-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0021

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2663
CVE	CVE-2022-3061
CVE	CVE-2022-3303
CVE	CVE-2022-3586
CVE	CVE-2022-3646
CVE	CVE-2022-39188
CVE	CVE-2022-4095

CVE	CVE-2022-20421
CVE	CVE-2022-39842
CVE	CVE-2022-40307
CVE	CVE-2022-43750
XREF	USN:5791-1

Plugin Information

Published: 2023/01/07, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-136-generic
 for this advisory.
```

171579 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5874-1 advisory.

It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3628)

It was discovered that a use-after-free vulnerability existed in the Bluetooth stack in the Linux kernel.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3640)

Khalid Masum discovered that the NILFS2 file system implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-3649)

It was discovered that a race condition existed in the SMSC UFX USB driver implementation in the Linux kernel, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41849)

It was discovered that a race condition existed in the Roccat HID driver in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41850)

Tams Koczka discovered that the Bluetooth L2CAP implementation in the Linux kernel did not properly initialize memory in some situations. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-42895)

It was discovered that the binder IPC implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-20928)

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

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

See Also

https://ubuntu.com/security/notices/USN-5874-1

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)

VPR Score

6.7

EPSS Score

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-3628
CVE	CVE-2022-3640
CVE	CVE-2022-3649
CVE	CVE-2022-41849
CVE	CVE-2022-41850
CVE	CVE-2022-42895
CVE	CVE-2023-20928
XREF	USN:5874-1

Plugin Information

Published: 2023/02/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-139-generic
 for this advisory.
```

172135 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory.

It was discovered that the Upper Level Protocol (ULP) subsystem in the Linux kernel did not properly handle sockets entering the LISTEN state in certain protocols, leading to a use-after-free vulnerability.

A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0461)

It was discovered that the NVMe driver in the Linux kernel did not properly handle reset events in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3169)

It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3424)

Gwangun Jung discovered a race condition in the IPv4 implementation in the Linux kernel when deleting multipath routes, resulting in an out-of-bounds read. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3435)

It was discovered that a race condition existed in the Kernel Connection Multiplexor (KCM) socket implementation in the Linux kernel when releasing sockets in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3521)

It was discovered that the Netronome Ethernet driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3545)

It was discovered that the hugetlb implementation in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2022-3623)

Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2022-36280)

Hyunwoo Kim discovered that the DVB Core driver in the Linux kernel did not properly perform reference counting in some situations, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41218)

It was discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-4139)

It was discovered that a race condition existed in the Xen network backend driver in the Linux kernel when handling dropped packets in certain circumstances. An attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-42328, CVE-2022-42329)

It was discovered that the Atmel WILC1000 driver in the Linux kernel did not properly validate offsets, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash). (CVE-2022-47520)

It was discovered that the network queuing discipline implementation in the Linux kernel contained a null pointer dereference in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-47929)

Jos Oliveira and Rodrigo Branco discovered that the prctl syscall implementation in the Linux kernel did not properly protect against indirect branch prediction attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-0045)

It was discovered that a use-after-free vulnerability existed in the Advanced Linux Sound Architecture (ALSA) subsystem. A local attacker could use this to cause a denial of service (system crash).

(CVE-2023-0266)

Kyle Zeng discovered that the IPv6 implementation in the Linux kernel contained a NULL pointer dereference vulnerability in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-0394)

It was discovered that the Android Binder IPC subsystem in the Linux kernel did not properly validate inputs in some situations, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-20938)

Kyle Zeng discovered that the class-based queuing discipline implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-23454)

Kyle Zeng discovered that the ATM VC queuing discipline implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-23455)

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

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

See Also

https://ubuntu.com/security/notices/USN-5917-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.0

EPSS Score

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-3169
CVE	CVE-2022-3424
CVE	CVE-2022-3435
CVE	CVE-2022-3521
CVE	CVE-2022-3545
CVE	CVE-2022-3623
CVE	CVE-2022-4139
CVE	CVE-2022-36280
CVE	CVE-2022-41218
CVE	CVE-2022-42328
CVE	CVE-2022-42329
CVE	CVE-2022-47520
CVE	CVE-2022-47929
CVE	CVE-2023-0045
CVE	CVE-2023-0266
CVE	CVE-2023-0394
CVE	CVE-2023-0461
CVE	CVE-2023-20938
CVE	CVE-2023-23454
CVE	CVE-2023-23455
XREF	USN:5917-1
XREF	CISA-KNOWN-EXPLOITED:2023/04/20

Plugin Information

Published: 2023/03/06, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-144-generic
 for this advisory.
```

174461 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory.

It was discovered that the Traffic-Control Index (TCINDEX) implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-1281)

Jiasheng Jiang discovered that the HSA Linux kernel driver for AMD Radeon GPU devices did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3108)

It was discovered that the infrared transceiver USB driver did not properly handle USB control messages. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3903)

Haowei Yan discovered that a race condition existed in the Layer 2 Tunneling Protocol (L2TP) implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-4129)

It was discovered that the Human Interface Device (HID) support driver in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1073)

It was discovered that a memory leak existed in the SCTP protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2023-1074)

Lianhui Tang discovered that the MPLS implementation in the Linux kernel did not properly handle certain sysctl allocation failure conditions, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-26545)

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

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

See Also

https://ubuntu.com/security/notices/USN-6027-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-3108
CVE	CVE-2022-3903
CVE	CVE-2022-4129
CVE	CVE-2023-1073
CVE	CVE-2023-1074
CVE	CVE-2023-1281
CVE	CVE-2023-26545
XREF	USN:6027-1

Plugin Information

Published: 2023/04/19, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-147-generic
 for this advisory.
```

176228 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory.

Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-3707)

Jordy Zomer and Alexandra Sandulescu discovered that the Linux kernel did not properly implement speculative execution barriers in usercopy functions in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2023-0459)

It was discovered that the TLS subsystem in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1075)

It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-1078)

Xingyuan Mo discovered that the x86 KVM implementation in the Linux kernel did not properly initialize some data structures. A local attacker could use this to expose sensitive information (kernel memory).

(CVE-2023-1513)

It was discovered that a use-after-free vulnerability existed in the iSCSI TCP implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash).

(CVE-2023-2162)

It was discovered that the NET/ROM protocol implementation in the Linux kernel contained a race condition in some situations, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32269)

Duoming Zhou discovered that a race condition existed in the infrared receiver/transceiver driver in the Linux kernel, leading to a use-after- free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-1118)

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

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

See Also

https://ubuntu.com/security/notices/USN-6094-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2022-3707
CVE	CVE-2023-0459
CVE	CVE-2023-1075
CVE	CVE-2023-1078
CVE	CVE-2023-1118
CVE	CVE-2023-1513
CVE	CVE-2023-2162
CVE	CVE-2023-32269
XREF	USN:6094-1

Plugin Information

Published: 2023/05/23, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-149-generic
 for this advisory.
```

176564 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory.

Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

(CVE-2023-32233)

Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-31436)

Reima Ishii discovered that the nested KVM implementation for Intel x86 processors in the Linux kernel did not properly validate control registers in certain situations. An attacker in a guest VM could use this to cause a denial of service (guest crash). (CVE-2023-30456)

It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform data buffer size validation in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1380)

Jean-Baptiste Cayrou discovered that the shiftfs file system in the Ubuntu Linux kernel contained a race condition when handling inode locking in some situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2612)

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

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

See Also

https://ubuntu.com/security/notices/USN-6131-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-1380
CVE	CVE-2023-2612
CVE	CVE-2023-30456
CVE	CVE-2023-31436
CVE	CVE-2023-32233
XREF	USN:6131-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2023/06/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-150-generic
 for this advisory.
```

190874 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6648-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6648-1 advisory.

It was discovered that a race condition existed in the AppleTalk networking subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51781)

Zhenghan Wang discovered that the generic ID allocator implementation in the Linux kernel did not properly check for null bitmap when releasing IDs. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-6915)

Robert Morris discovered that the CIFS network file system implementation in the Linux kernel did not properly validate certain server commands fields, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2024-0565)

Jann Horn discovered that the TLS subsystem in the Linux kernel did not properly handle spliced messages, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-0646)

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

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

See Also

https://ubuntu.com/security/notices/USN-6648-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-6915
CVE	CVE-2023-51781
CVE	CVE-2024-0565
CVE	CVE-2024-0646
XREF	USN:6648-1

Plugin Information

Published: 2024/02/22, Modified: 2024/08/28

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-172-generic
 for this advisory.
```

191663 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6681-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6681-1 advisory.

Wenqing Liu discovered that the f2fs file system implementation in the Linux kernel did not properly validate inode types while performing garbage collection. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash).

(CVE-2021-44879)

It was discovered that the DesignWare USB3 for Qualcomm SoCs driver in the Linux kernel did not properly handle certain error conditions during device registration. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-22995)

Bien Pham discovered that the netfiler subsystem in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4244)

It was discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51779)

It was discovered that a race condition existed in the ATM (Asynchronous Transfer Mode) subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51780)

It was discovered that a race condition existed in the Rose X.25 protocol implementation in the Linux kernel, leading to a use-after- free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-51782)

Alon Zahavi discovered that the NVMe-oF/TCP subsystem of the Linux kernel did not properly handle connect command payloads in certain situations, leading to an out-of-bounds read vulnerability. A remote attacker could use this to expose sensitive information (kernel memory). (CVE-2023-6121)

It was discovered that the VirtIO subsystem in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to possibly expose sensitive information (kernel memory).

(CVE-2024-0340)

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

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

See Also

https://ubuntu.com/security/notices/USN-6681-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0018

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-44879
CVE	CVE-2023-4244
CVE	CVE-2023-6121
CVE	CVE-2023-22995
CVE	CVE-2023-51779
CVE	CVE-2023-51780
CVE	CVE-2023-51782
CVE	CVE-2024-0340
XREF	USN:6681-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-173-generic
 for this advisory.
```

192292 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6702-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6702-1 advisory.

It was discovered that the NVIDIA Tegra XUSB pad controller driver in the Linux kernel did not properly handle return values in certain error conditions. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-23000)

It was discovered that the ARM Mali Display Processor driver implementation in the Linux kernel did not properly handle certain error conditions. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-23004)

Notselwyn discovered that the netfilter subsystem in the Linux kernel did not properly handle verdict parameters in certain cases, leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-1086)

It was discovered that a race condition existed in the SCSI Emulex LightPulse Fibre Channel driver in the Linux kernel when unregistering FCF and re-scanning an HBA FCF table, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash).

(CVE-2024-24855)

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

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

See Also

https://ubuntu.com/security/notices/USN-6702-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.6

EPSS Score

0.0029

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-23000
CVE	CVE-2023-23004
CVE	CVE-2024-1086
CVE	CVE-2024-24855
XREF	USN:6702-1
XREF	CISA-KNOWN-EXPLOITED:2024/06/20

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-174-generic
 for this advisory.
```

193081 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6726-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6726-1 advisory.

Pratyush Yadav discovered that the Xen network backend implementation in the Linux kernel did not properly handle zero length data request, leading to a null pointer dereference vulnerability. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2023-46838)

It was discovered that the IPv6 implementation of the Linux kernel did not properly manage route cache memory usage. A remote attacker could use this to cause a denial of service (memory exhaustion).

(CVE-2023-52340)

It was discovered that the device mapper driver in the Linux kernel did not properly validate target size during certain memory allocations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-52429, CVE-2024-23851)

Dan Carpenter discovered that the netfilter subsystem in the Linux kernel did not store data in properly sized memory locations. A local user could use this to cause a denial of service (system crash).

(CVE-2024-0607)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Architecture specifics;

- Cryptographic API;

- Android drivers;

- EDAC drivers;

- GPU drivers;

- Media drivers;

- MTD block device drivers;

- Network drivers;

- NVME drivers;

- TTY drivers;

- Userspace I/O drivers;

- F2FS file system;

- GFS2 file system;

- IPv6 Networking;

- AppArmor security module; (CVE-2023-52464, CVE-2023-52448, CVE-2023-52457, CVE-2023-52443, CVE-2023-52439, CVE-2023-52612, CVE-2024-26633, CVE-2024-26597, CVE-2023-52449, CVE-2023-52444, CVE-2023-52609, CVE-2023-52469, CVE-2023-52445, CVE-2023-52451, CVE-2023-52470, CVE-2023-52454, CVE-2023-52436, CVE-2023-52438)

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

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

See Also

https://ubuntu.com/security/notices/USN-6726-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-46838
CVE	CVE-2023-52340
CVE	CVE-2023-52429
CVE	CVE-2023-52436
CVE	CVE-2023-52438
CVE	CVE-2023-52439
CVE	CVE-2023-52443
CVE	CVE-2023-52444
CVE	CVE-2023-52445
CVE	CVE-2023-52448
CVE	CVE-2023-52449
CVE	CVE-2023-52451
CVE	CVE-2023-52454
CVE	CVE-2023-52457
CVE	CVE-2023-52464
CVE	CVE-2023-52469
CVE	CVE-2023-52470
CVE	CVE-2023-52609
CVE	CVE-2023-52612
CVE	CVE-2024-0607
CVE	CVE-2024-23851
CVE	CVE-2024-26597
CVE	CVE-2024-26633
XREF	USN:6726-1

Plugin Information

Published: 2024/04/09, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-175-generic
 for this advisory.
```

193596 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6741-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6741-1 advisory.

Daniele Antonioli discovered that the Secure Simple Pairing and Secure Connections pairing in the Bluetooth protocol could allow an unauthenticated user to complete authentication without pairing credentials. A physically proximate attacker placed between two Bluetooth devices could use this to subsequently impersonate one of the paired devices. (CVE-2023-24023)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- JFS file system;

- BPF subsystem;

- Netfilter; (CVE-2023-52603, CVE-2023-52600, CVE-2024-26581, CVE-2024-26589)

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

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

See Also

https://ubuntu.com/security/notices/USN-6741-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.0033

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-2023-24023
CVE	CVE-2023-52600
CVE	CVE-2023-52603
CVE	CVE-2024-26581
CVE	CVE-2024-26589
XREF	USN:6741-1

Plugin Information

Published: 2024/04/19, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-177-generic
 for this advisory.
```

195135 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6767-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6767-1 advisory.

Chenyuan Yang discovered that the RDS Protocol implementation in the Linux kernel contained an out-of-bounds read vulnerability. An attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-23849)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;

- PowerPC architecture;

- S390 architecture;

- Block layer subsystem;

- Android drivers;

- Hardware random number generator core;

- GPU drivers;

- Hardware monitoring drivers;

- I2C subsystem;

- IIO Magnetometer sensors drivers;

- InfiniBand drivers;

- Network drivers;

- PCI driver for MicroSemi Switchtec;

- PHY drivers;

- Ceph distributed file system;

- Ext4 file system;

- JFS file system;

- NILFS2 file system;

- Pstore file system;

- Core kernel;

- Memory management;

- CAN network layer;

- Networking core;

- IPv4 networking;

- Logical Link layer;

- Netfilter;

- NFC subsystem;

- SMC sockets;

- Sun RPC protocol;

- TIPC protocol;

- Realtek audio codecs; (CVE-2024-26696, CVE-2023-52583, CVE-2024-26720, CVE-2023-52615, CVE-2023-52599, CVE-2023-52587, CVE-2024-26635, CVE-2024-26704, CVE-2024-26625, CVE-2024-26825, CVE-2023-52622, CVE-2023-52435, CVE-2023-52617, CVE-2023-52598, CVE-2024-26645, CVE-2023-52619, CVE-2024-26593, CVE-2024-26685, CVE-2023-52602, CVE-2023-52486, CVE-2024-26697, CVE-2024-26675, CVE-2024-26600, CVE-2023-52604, CVE-2024-26664, CVE-2024-26606, CVE-2023-52594, CVE-2024-26671, CVE-2024-26598, CVE-2024-26673, CVE-2024-26920, CVE-2024-26722, CVE-2023-52601, CVE-2024-26602, CVE-2023-52637, CVE-2023-52623, CVE-2024-26702, CVE-2023-52597, CVE-2024-26684, CVE-2023-52606, CVE-2024-26679, CVE-2024-26663, CVE-2024-26910, CVE-2024-26615, CVE-2023-52595, CVE-2023-52607, CVE-2024-26636)

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

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

See Also

https://ubuntu.com/security/notices/USN-6767-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2023-52435
CVE	CVE-2023-52486
CVE	CVE-2023-52583
CVE	CVE-2023-52587
CVE	CVE-2023-52594
CVE	CVE-2023-52595
CVE	CVE-2023-52597
CVE	CVE-2023-52598
CVE	CVE-2023-52599
CVE	CVE-2023-52601
CVE	CVE-2023-52602
CVE	CVE-2023-52604
CVE	CVE-2023-52606
CVE	CVE-2023-52607
CVE	CVE-2023-52615
CVE	CVE-2023-52617
CVE	CVE-2023-52619
CVE	CVE-2023-52622
CVE	CVE-2023-52623
CVE	CVE-2023-52637
CVE	CVE-2024-23849
CVE	CVE-2024-26593
CVE	CVE-2024-26598
CVE	CVE-2024-26600
CVE	CVE-2024-26602
CVE	CVE-2024-26606
CVE	CVE-2024-26615

CVE	CVE-2024-26625
CVE	CVE-2024-26635
CVE	CVE-2024-26636
CVE	CVE-2024-26645
CVE	CVE-2024-26663
CVE	CVE-2024-26664
CVE	CVE-2024-26671
CVE	CVE-2024-26673
CVE	CVE-2024-26675
CVE	CVE-2024-26679
CVE	CVE-2024-26684
CVE	CVE-2024-26685
CVE	CVE-2024-26696
CVE	CVE-2024-26697
CVE	CVE-2024-26702
CVE	CVE-2024-26704
CVE	CVE-2024-26720
CVE	CVE-2024-26722
CVE	CVE-2024-26825
CVE	CVE-2024-26910
CVE	CVE-2024-26920
XREF	USN:6767-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-181-generic
 for this advisory.
```

200450 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6831-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6831-1 advisory.

It was discovered that the HugeTLB file system component of the Linux Kernel contained a NULL pointer dereference vulnerability. A privileged attacker could possibly use this to to cause a denial of service.

(CVE-2024-0841)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;

- PowerPC architecture;

- x86 architecture;

- DMA engine subsystem;

- EFI core;

- GPU drivers;

- InfiniBand drivers;

- Multiple devices driver;

- Network drivers;

- Power supply drivers;

- TCM subsystem;

- Userspace I/O drivers;

- USB subsystem;

- Framebuffer layer;

- AFS file system;

- File systems infrastructure;

- BTRFS file system;

- Ext4 file system;

- Bluetooth subsystem;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- L2TP protocol;

- MAC80211 subsystem;

- Netfilter;

- Netlink;

- Wireless networking; (CVE-2024-26748, CVE-2024-27417, CVE-2024-26840, CVE-2023-52504, CVE-2024-26790, CVE-2024-26763, CVE-2024-26805, CVE-2024-26773, CVE-2021-47063, CVE-2024-26791, CVE-2024-27413, CVE-2024-26788, CVE-2024-27405, CVE-2024-26845, CVE-2024-26766, CVE-2021-47070, CVE-2024-26839, CVE-2024-26712, CVE-2024-27412, CVE-2024-26752, CVE-2024-26778, CVE-2024-26735, CVE-2024-26736, CVE-2024-27410, CVE-2024-26779, CVE-2024-26804, CVE-2024-26749, CVE-2024-26793, CVE-2024-26764, CVE-2024-26751, CVE-2024-35811, CVE-2024-26835, CVE-2024-26772, CVE-2024-26777, CVE-2024-26688, CVE-2024-27416, CVE-2024-26801, CVE-2024-26733, CVE-2024-27414, CVE-2024-26754, CVE-2024-26848)

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

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

See Also

https://ubuntu.com/security/notices/USN-6831-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0005

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-2021-47063
CVE	CVE-2021-47070
CVE	CVE-2023-52504
CVE	CVE-2024-0841
CVE	CVE-2024-26688
CVE	CVE-2024-26712
CVE	CVE-2024-26733
CVE	CVE-2024-26735
CVE	CVE-2024-26736
CVE	CVE-2024-26748
CVE	CVE-2024-26749
CVE	CVE-2024-26751
CVE	CVE-2024-26752
CVE	CVE-2024-26754
CVE	CVE-2024-26763
CVE	CVE-2024-26764
CVE	CVE-2024-26766
CVE	CVE-2024-26772
CVE	CVE-2024-26773
CVE	CVE-2024-26777
CVE	CVE-2024-26778
CVE	CVE-2024-26779
CVE	CVE-2024-26788
CVE	CVE-2024-26790
CVE	CVE-2024-26791
CVE	CVE-2024-26793
CVE	CVE-2024-26801
CVE	CVE-2024-26804
CVE	CVE-2024-26805
CVE	CVE-2024-26835
CVE	CVE-2024-26839
CVE	CVE-2024-26840
CVE	CVE-2024-26845
CVE	CVE-2024-26848

CVE	CVE-2024-27405
CVE	CVE-2024-27410
CVE	CVE-2024-27412
CVE	CVE-2024-27413
CVE	CVE-2024-27414
CVE	CVE-2024-27416
CVE	CVE-2024-27417
CVE	CVE-2024-35811
XREF	USN:6831-1

Plugin Information

Published: 2024/06/12, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-186-generic
 for this advisory.
```

201871 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6868-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6868-1 advisory.

Sander Wiebing, Alvise de Faveri Tron, Herbert Bos, and Cristiano Giuffrida discovered that the Linux kernel mitigations for the initial Branch History Injection vulnerability (CVE-2022-0001) were insufficient for Intel processors. A local attacker could potentially use this to expose sensitive information. (CVE-2024-2201)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Netfilter; (CVE-2024-26925, CVE-2024-26643)

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

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

See Also

https://ubuntu.com/security/notices/USN-6868-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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)

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.0 (CVSS2#AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-2201
CVE	CVE-2024-26643
CVE	CVE-2024-26925
XREF	USN:6868-1

Plugin Information

Published: 2024/07/04, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-187-generic
 for this advisory.
```

204835 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6924-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6924-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM SCMI message protocol;

- InfiniBand drivers;

- TTY drivers;

- TLS protocol; (CVE-2024-26584, CVE-2024-36016, CVE-2024-26585, CVE-2021-47131, CVE-2024-26907, CVE-2022-48655, CVE-2024-26583)

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

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

See Also

https://ubuntu.com/security/notices/USN-6924-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-47131
CVE	CVE-2022-48655
CVE	CVE-2024-26583
CVE	CVE-2024-26584
CVE	CVE-2024-26585
CVE	CVE-2024-26907
CVE	CVE-2024-36016
XREF	USN:6924-1

Plugin Information

Published: 2024/07/29, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-190-generic
 for this advisory.
```

205223 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6951-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;

- M68K architecture;

- User-Mode Linux (UML);

- x86 architecture;

- Accessibility subsystem;

- Character device driver;

- Clock framework and drivers;

- CPU frequency scaling framework;

- Hardware crypto device drivers;

- Buffer Sharing and Synchronization framework;

- FireWire subsystem;

- GPU drivers;

- HW tracing;

- Macintosh device drivers;

- Multiple devices driver;

- Media drivers;

- Network drivers;

- Pin controllers subsystem;

- S/390 drivers;

- SCSI drivers;

- SoundWire subsystem;

- Greybus lights staging drivers;

- TTY drivers;
- Framebuffer layer;
- Virtio drivers;
- 9P distributed file system;
- eCrypt file system;
- EROFS file system;
- Ext4 file system;
- F2FS file system;
- JFFS2 file system;
- Network file system client;
- NILFS2 file system;
- SMB network file system;
- Kernel debugger infrastructure;
- IRQ subsystem;
- Tracing infrastructure;
- Dynamic debug library;
- 9P file system network protocol;
- Bluetooth subsystem;
- Networking core;
- IPv4 networking;
- IPv6 networking;
- Netfilter;
- NET/ROM layer;
- NFC subsystem;
- NSH protocol;
- Open vSwitch;
- Phonet protocol;
- TIPC protocol;
- Unix domain sockets;
- Wireless networking;
- eXpress Data Path;

- XFRM subsystem;

- ALSA framework; (CVE-2024-36934, CVE-2024-38578, CVE-2024-38600, CVE-2024-27399, CVE-2024-39276, CVE-2024-38596, CVE-2024-36933, CVE-2024-36919, CVE-2024-35976, CVE-2024-37356, CVE-2023-52585, CVE-2024-38558, CVE-2024-38560, CVE-2024-38634, CVE-2024-36959, CVE-2024-38633, CVE-2024-36886, CVE-2024-27398, CVE-2024-39493, CVE-2024-26886, CVE-2024-31076, CVE-2024-38559, CVE-2024-38615, CVE-2024-36971, CVE-2024-38627, CVE-2024-36964, CVE-2024-38780, CVE-2024-37353, CVE-2024-38621, CVE-2024-36883, CVE-2024-39488, CVE-2024-38661, CVE-2024-36939, CVE-2024-38589, CVE-2024-38565, CVE-2024-38381, CVE-2024-35947, CVE-2024-36905, CVE-2022-48772, CVE-2024-36017, CVE-2024-36946, CVE-2024-27401, CVE-2024-38579, CVE-2024-38612, CVE-2024-38598, CVE-2024-38635, CVE-2024-38587, CVE-2024-38567, CVE-2024-38549, CVE-2024-36960, CVE-2023-52752, CVE-2024-27019, CVE-2024-38601, CVE-2024-39489, CVE-2024-39467, CVE-2023-52882, CVE-2024-38583, CVE-2024-39480, CVE-2024-38607, CVE-2024-36940, CVE-2024-38659, CVE-2023-52434, CVE-2024-36015, CVE-2024-38582, CVE-2024-36950, CVE-2024-38552, CVE-2024-33621, CVE-2024-36954, CVE-2024-39475, CVE-2024-39301, CVE-2024-38599, CVE-2024-36902, CVE-2024-36286, CVE-2024-38613, CVE-2024-38637, CVE-2024-36941, CVE-2024-36014, CVE-2024-38618, CVE-2024-36904, CVE-2024-36270, CVE-2024-39292, CVE-2024-39471, CVE-2022-48674)

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

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

See Also

https://ubuntu.com/security/notices/USN-6951-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-48674
CVE	CVE-2022-48772
CVE	CVE-2023-52434
CVE	CVE-2023-52585
CVE	CVE-2023-52752
CVE	CVE-2023-52882
CVE	CVE-2024-26886
CVE	CVE-2024-27019
CVE	CVE-2024-27398
CVE	CVE-2024-27399
CVE	CVE-2024-27401
CVE	CVE-2024-31076
CVE	CVE-2024-33621
CVE	CVE-2024-35947
CVE	CVE-2024-35976
CVE	CVE-2024-36014
CVE	CVE-2024-36015
CVE	CVE-2024-36017
CVE	CVE-2024-36270
CVE	CVE-2024-36286
CVE	CVE-2024-36883
CVE	CVE-2024-36886
CVE	CVE-2024-36902
CVE	CVE-2024-36904
CVE	CVE-2024-36905
CVE	CVE-2024-36919
CVE	CVE-2024-36933
CVE	CVE-2024-36934
CVE	CVE-2024-36939
CVE	CVE-2024-36940
CVE	CVE-2024-36941
CVE	CVE-2024-36946
CVE	CVE-2024-36950
CVE	CVE-2024-36954
CVE	CVE-2024-36959
CVE	CVE-2024-36960

CVE	CVE-2024-36964
CVE	CVE-2024-36971
CVE	CVE-2024-37353
CVE	CVE-2024-37356
CVE	CVE-2024-38381
CVE	CVE-2024-38549
CVE	CVE-2024-38552
CVE	CVE-2024-38558
CVE	CVE-2024-38559
CVE	CVE-2024-38560
CVE	CVE-2024-38565
CVE	CVE-2024-38567
CVE	CVE-2024-38578
CVE	CVE-2024-38579
CVE	CVE-2024-38582
CVE	CVE-2024-38583
CVE	CVE-2024-38587
CVE	CVE-2024-38589
CVE	CVE-2024-38596
CVE	CVE-2024-38598
CVE	CVE-2024-38599
CVE	CVE-2024-38600
CVE	CVE-2024-38601
CVE	CVE-2024-38607
CVE	CVE-2024-38612
CVE	CVE-2024-38613
CVE	CVE-2024-38615
CVE	CVE-2024-38618
CVE	CVE-2024-38621
CVE	CVE-2024-38627
CVE	CVE-2024-38633
CVE	CVE-2024-38634
CVE	CVE-2024-38635
CVE	CVE-2024-38637
CVE	CVE-2024-38659
CVE	CVE-2024-38661
CVE	CVE-2024-38780
CVE	CVE-2024-39276
CVE	CVE-2024-39292
CVE	CVE-2024-39301
CVE	CVE-2024-39467
CVE	CVE-2024-39471
CVE	CVE-2024-39475

CVE	CVE-2024-39480
CVE	CVE-2024-39488
CVE	CVE-2024-39489
CVE	CVE-2024-39493
XREF	CISA-KNOWN-EXPLOITED:2024/08/28
XREF	USN:6951-1

Plugin Information

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

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-192-generic
 for this advisory.
```

206077 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6973-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6973-1 advisory.

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel, leading to a null pointer dereference vulnerability. A privileged local attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-24860)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- SuperH RISC architecture;

- MMC subsystem;

- Network drivers;

- SCSI drivers;

- GFS2 file system;

- IPv4 networking;

- IPv6 networking;

- HD-audio driver; (CVE-2024-26830, CVE-2024-39484, CVE-2024-36901, CVE-2024-26929, CVE-2024-26921, CVE-2021-46926, CVE-2023-52629, CVE-2023-52760)

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

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

See Also

https://ubuntu.com/security/notices/USN-6973-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-46926
CVE	CVE-2023-52629
CVE	CVE-2023-52760
CVE	CVE-2024-24860
CVE	CVE-2024-26830
CVE	CVE-2024-26921
CVE	CVE-2024-26929
CVE	CVE-2024-36901
CVE	CVE-2024-39484
XREF	USN:6973-1

Plugin Information

Published: 2024/08/21, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-193-generic
 for this advisory.
```

207398 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7022-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-7022-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- GPU drivers;

- Modular ISDN driver;

- MMC subsystem;

- SCSI drivers;

- F2FS file system;

- GFS2 file system;

- Netfilter;

- RxRPC session sockets;

- Integrity Measurement Architecture(IMA) framework; (CVE-2021-47188, CVE-2024-27012, CVE-2024-42228, CVE-2022-48791, CVE-2024-39494, CVE-2022-48863, CVE-2024-26787, CVE-2024-42160, CVE-2024-38570, CVE-2024-26677)

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

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

See Also

https://ubuntu.com/security/notices/USN-7022-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-47188
CVE	CVE-2022-48791
CVE	CVE-2022-48863
CVE	CVE-2024-26677
CVE	CVE-2024-26787
CVE	CVE-2024-27012
CVE	CVE-2024-38570
CVE	CVE-2024-39494
CVE	CVE-2024-42160
CVE	CVE-2024-42228
XREF	USN:7022-1

Plugin Information

Published: 2024/09/18, Modified: 2024/09/18

Plugin Output

tcp/0

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

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-196-generic
 for this advisory.
```

156879 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5240-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5240-1 advisory.

William Liu and Jamie Hill-Daniel discovered that the file system context functionality in the Linux kernel contained an integer underflow vulnerability, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-5240-1

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0024

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0185
XREF	USN:5240-1
XREF	CISA-KNOWN-EXPLOITED:2024/09/11

Exploitable With

Core Impact (true)

Plugin Information

Published: 2022/01/20, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-96-generic
 for this advisory.
```

204962 - Ubuntu 18.04 LTS : Bind vulnerabilities (USN-6909-2)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6909-2 advisory.

USN-6909-1 fixed several vulnerabilities in Bind. This update provides the corresponding update for Ubuntu 18.04 LTS.

Original advisory details:

Toshifumi Sakaguchi discovered that Bind incorrectly handled having a very

large number of RRs existing at the same time. A remote attacker could

possibly use this issue to cause Bind to consume resources, leading to a

denial of service. (CVE-2024-1737)

It was discovered that Bind incorrectly handled a large number of SIG(0)

signed requests. A remote attacker could possibly use this issue to cause

Bind to consume resources, leading to a denial of service. (CVE-2024-1975)

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

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

See Also

https://ubuntu.com/security/notices/USN-6909-2

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)

VPR Score

3.6

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-1737
CVE	CVE-2024-1975
XREF	IAVA:2024-A-0442
XREF	USN:6909-2

Plugin Information

Published: 2024/08/01, 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 : bind9-host_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : bind9-host_1:9.11.3+dfsg-1ubuntu1.19+esm4

  - Installed package : dnsutils_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : dnsutils_1:9.11.3+dfsg-1ubuntu1.19+esm4

  - Installed package : libbind9-160_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libbind9-160_1:9.11.3+dfsg-1ubuntu1.19+esm4

  - Installed package : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.18
  - Fixed package     : libdns-export1100_1:9.11.3+dfsg-1ubuntu1.19+esm4
```

```
- Installed package : libdns1100_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libdns1100_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : libirs160_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libirs160_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : libisc-export169_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libisc-export169_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : libisc169_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libisc169_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : libisccc160_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libisccc160_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : libisccfg160_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : libisccfg160_1:9.11.3+dfsg-1ubuntu1.19+esm4

- Installed package : liblwres160_1:9.11.3+dfsg-1ubuntu1.18
- Fixed package     : liblwres160_1:9.11.3+dfsg-1ubuntu1.19+esm4
```

173652 - Ubuntu 18.04 LTS : Linux kernel vulnerabilities (USN-5985-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5985-1 advisory.

It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service (memory exhaustion).

(CVE-2021-3669)

It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. (CVE-2022-2196)

Gerald Lee discovered that the USB Gadget file system implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-4382)

It was discovered that the RNDIS USB driver in the Linux kernel contained an integer overflow vulnerability. A local attacker with physical access could plug in a malicious USB device to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-23559)

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

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

See Also

https://ubuntu.com/security/notices/USN-5985-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0007

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-2021-3669
CVE	CVE-2022-2196
CVE	CVE-2022-4382
CVE	CVE-2023-23559
XREF	USN:5985-1

Plugin Information

Published: 2023/03/29, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-146-generic
 for this advisory.
```

202478 - Ubuntu 18.04 LTS : Linux kernel vulnerabilities (USN-6896-2)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6896-2 advisory.

It was discovered that the ATA over Ethernet (AoE) driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6270)

It was discovered that the Atheros 802.11ac wireless driver did not properly validate certain data structures, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service. (CVE-2023-7042)

Yuxuan Hu discovered that the Bluetooth RFCOMM protocol driver in the Linux Kernel contained a race condition, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-22099)

Gui-Dong Han discovered that the software RAID driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. A privileged attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-23307)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel when modifying certain settings values through debugfs. A privileged local attacker could use this to cause a denial of service. (CVE-2024-24857, CVE-2024-24858, CVE-2024-24859)

Bai Jiaju discovered that the Xceive XC4000 silicon tuner device driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-24861)

Chenyuan Yang discovered that the Unsorted Block Images (UBI) flash device volume management subsystem did not properly validate logical eraseblock sizes in certain situations. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-25739)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- x86 architecture;

- Block layer subsystem;

- Accessibility subsystem;

- ACPI drivers;

- Android drivers;

- Bluetooth drivers;

- Clock framework and drivers;

- Data acquisition framework and drivers;

- Cryptographic API;
- GPU drivers;
- HID subsystem;
- I2C subsystem;
- IRQ chip drivers;
- Multiple devices driver;
- Media drivers;
- VMware VMCI Driver;
- MMC subsystem;
- Network drivers;
- PCI subsystem;
- SCSI drivers;
- Freescale SoC drivers;
- SPI subsystem;
- Media staging drivers;
- TTY drivers;
- USB subsystem;
- VFIO drivers;
- Framebuffer layer;
- Xen hypervisor drivers;
- File systems infrastructure;
- BTRFS file system;
- Ext4 file system;
- FAT file system;
- NILFS2 file system;
- Diskquota system;
- SMB network file system;
- UBI file system;
- io_uring subsystem;
- BPF subsystem;
- Core kernel;

- Memory management;

- B.A.T.M.A.N. meshing protocol;

- Bluetooth subsystem;

- Networking core;

- HSR network protocol;

- IPv4 networking;

- IPv6 networking;

- MAC80211 subsystem;

- Netfilter;

- NET/ROM layer;

- NFC subsystem;

- Open vSwitch;

- Packet sockets;

- RDS protocol;

- Network traffic control;

- Sun RPC protocol;

- Unix domain sockets;

- ALSA SH drivers;

- USB sound devices;

- KVM core; (CVE-2024-27076, CVE-2024-35849, CVE-2024-35899, CVE-2024-27038, CVE-2024-35982, CVE-2024-26687, CVE-2024-26863, CVE-2024-36004, CVE-2024-27004, CVE-2024-27065, CVE-2024-36020, CVE-2024-27000, CVE-2024-26981, CVE-2024-26973, CVE-2024-35922, CVE-2024-35969, CVE-2024-26851, CVE-2023-52880, CVE-2024-35813, CVE-2024-26859, CVE-2024-27078, CVE-2024-27020, CVE-2024-35809, CVE-2024-27001, CVE-2024-26969, CVE-2024-26993, CVE-2024-35935, CVE-2024-35815, CVE-2024-26931, CVE-2024-35823, CVE-2024-26984, CVE-2024-27024, CVE-2024-27419, CVE-2024-27008, CVE-2024-35825, CVE-2023-52644, CVE-2024-35933, CVE-2024-35830, CVE-2024-35900, CVE-2024-27046, CVE-2024-26651, CVE-2024-27013, CVE-2024-27437, CVE-2024-26966, CVE-2024-26974, CVE-2024-26889, CVE-2024-26862, CVE-2024-27043, CVE-2024-35852, CVE-2024-35821, CVE-2024-35886, CVE-2024-35888, CVE-2023-52699, CVE-2024-35997, CVE-2024-26586, CVE-2024-35898, CVE-2024-26934, CVE-2024-35915, CVE-2024-35897, CVE-2024-35973, CVE-2024-27028, CVE-2024-26874, CVE-2024-26923, CVE-2024-26937, CVE-2024-26857, CVE-2024-26855, CVE-2024-35893, CVE-2024-26810, CVE-2024-35910, CVE-2024-26820, CVE-2024-27075, CVE-2024-26816, CVE-2024-26642, CVE-2024-35936, CVE-2024-27073, CVE-2024-35853, CVE-2024-26965, CVE-2023-52650, CVE-2024-27396, CVE-2024-26999, CVE-2024-35855, CVE-2024-26880, CVE-2024-26901, CVE-2024-26894, CVE-2024-26884, CVE-2024-35950, CVE-2024-26957, CVE-2024-27395, CVE-2024-35819, CVE-2024-35978, CVE-2024-36007, CVE-2024-35805, CVE-2024-27436, CVE-2023-52620, CVE-2023-52656, CVE-2024-36006, CVE-2024-35877, CVE-2024-26898, CVE-2024-26935, CVE-2024-35828, CVE-2024-26875, CVE-2024-26654, CVE-2024-35930, CVE-2024-26817, CVE-2024-27388, CVE-2024-26828, CVE-2024-35984, CVE-2024-26812, CVE-2024-35807, CVE-2024-35854, CVE-2024-26878, CVE-2024-26883, CVE-2024-27077, CVE-2024-26922, CVE-2024-27059, CVE-2024-35955, CVE-2024-26903, CVE-2024-35895, CVE-2024-35925, CVE-2024-26882, CVE-2022-48627, CVE-2024-35847, CVE-2024-26813, CVE-2024-26994, CVE-2024-35806,

CVE-2024-26926, CVE-2024-35822, CVE-2024-27074, CVE-2024-26976, CVE-2024-26955, CVE-2024-27044, CVE-2024-35789, CVE-2024-27030, CVE-2024-26852, CVE-2024-27053, CVE-2024-35960, CVE-2024-26956, CVE-2024-35944)

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

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

See Also

https://ubuntu.com/security/notices/USN-6896-2

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

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-48627
CVE	CVE-2023-6270
CVE	CVE-2023-7042

CVE	CVE-2023-52620
CVE	CVE-2023-52644
CVE	CVE-2023-52650
CVE	CVE-2023-52656
CVE	CVE-2023-52699
CVE	CVE-2023-52880
CVE	CVE-2024-22099
CVE	CVE-2024-23307
CVE	CVE-2024-24857
CVE	CVE-2024-24858
CVE	CVE-2024-24859
CVE	CVE-2024-24861
CVE	CVE-2024-25739
CVE	CVE-2024-26586
CVE	CVE-2024-26642
CVE	CVE-2024-26651
CVE	CVE-2024-26654
CVE	CVE-2024-26687
CVE	CVE-2024-26810
CVE	CVE-2024-26812
CVE	CVE-2024-26813
CVE	CVE-2024-26816
CVE	CVE-2024-26817
CVE	CVE-2024-26820
CVE	CVE-2024-26828
CVE	CVE-2024-26851
CVE	CVE-2024-26852
CVE	CVE-2024-26855
CVE	CVE-2024-26857
CVE	CVE-2024-26859
CVE	CVE-2024-26862
CVE	CVE-2024-26863
CVE	CVE-2024-26874
CVE	CVE-2024-26875
CVE	CVE-2024-26878
CVE	CVE-2024-26880
CVE	CVE-2024-26882
CVE	CVE-2024-26883
CVE	CVE-2024-26884
CVE	CVE-2024-26889
CVE	CVE-2024-26894
CVE	CVE-2024-26898
CVE	CVE-2024-26901

CVE	CVE-2024-26903
CVE	CVE-2024-26922
CVE	CVE-2024-26923
CVE	CVE-2024-26926
CVE	CVE-2024-26931
CVE	CVE-2024-26934
CVE	CVE-2024-26935
CVE	CVE-2024-26937
CVE	CVE-2024-26955
CVE	CVE-2024-26956
CVE	CVE-2024-26957
CVE	CVE-2024-26965
CVE	CVE-2024-26966
CVE	CVE-2024-26969
CVE	CVE-2024-26973
CVE	CVE-2024-26974
CVE	CVE-2024-26976
CVE	CVE-2024-26981
CVE	CVE-2024-26984
CVE	CVE-2024-26993
CVE	CVE-2024-26994
CVE	CVE-2024-26999
CVE	CVE-2024-27000
CVE	CVE-2024-27001
CVE	CVE-2024-27004
CVE	CVE-2024-27008
CVE	CVE-2024-27013
CVE	CVE-2024-27020
CVE	CVE-2024-27024
CVE	CVE-2024-27028
CVE	CVE-2024-27030
CVE	CVE-2024-27038
CVE	CVE-2024-27043
CVE	CVE-2024-27044
CVE	CVE-2024-27046
CVE	CVE-2024-27053
CVE	CVE-2024-27059
CVE	CVE-2024-27065
CVE	CVE-2024-27073
CVE	CVE-2024-27074
CVE	CVE-2024-27075
CVE	CVE-2024-27076
CVE	CVE-2024-27077

CVE	CVE-2024-27078
CVE	CVE-2024-27388
CVE	CVE-2024-27395
CVE	CVE-2024-27396
CVE	CVE-2024-27419
CVE	CVE-2024-27436
CVE	CVE-2024-27437
CVE	CVE-2024-35789
CVE	CVE-2024-35805
CVE	CVE-2024-35806
CVE	CVE-2024-35807
CVE	CVE-2024-35809
CVE	CVE-2024-35813
CVE	CVE-2024-35815
CVE	CVE-2024-35819
CVE	CVE-2024-35821
CVE	CVE-2024-35822
CVE	CVE-2024-35823
CVE	CVE-2024-35825
CVE	CVE-2024-35828
CVE	CVE-2024-35830
CVE	CVE-2024-35847
CVE	CVE-2024-35849
CVE	CVE-2024-35852
CVE	CVE-2024-35853
CVE	CVE-2024-35854
CVE	CVE-2024-35855
CVE	CVE-2024-35877
CVE	CVE-2024-35886
CVE	CVE-2024-35888
CVE	CVE-2024-35893
CVE	CVE-2024-35895
CVE	CVE-2024-35897
CVE	CVE-2024-35898
CVE	CVE-2024-35899
CVE	CVE-2024-35900
CVE	CVE-2024-35910
CVE	CVE-2024-35915
CVE	CVE-2024-35922
CVE	CVE-2024-35925
CVE	CVE-2024-35930
CVE	CVE-2024-35933
CVE	CVE-2024-35935

CVE	CVE-2024-35936
CVE	CVE-2024-35944
CVE	CVE-2024-35950
CVE	CVE-2024-35955
CVE	CVE-2024-35960
CVE	CVE-2024-35969
CVE	CVE-2024-35973
CVE	CVE-2024-35978
CVE	CVE-2024-35982
CVE	CVE-2024-35984
CVE	CVE-2024-35997
CVE	CVE-2024-36004
CVE	CVE-2024-36006
CVE	CVE-2024-36007
CVE	CVE-2024-36020
XREF	USN:6896-2

Plugin Information

Published: 2024/07/16, 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.

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-189-generic
 for this advisory.
```

201049 - Ubuntu 18.04 LTS : SQLite vulnerability (USN-6566-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6566-2 advisory.

USN-6566-1 fixed several vulnerabilities in SQLite. This update provides the corresponding fix for CVE-2023-7104 for Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that SQLite incorrectly handled certain memory operations in the sessions extension. A remote attacker could possibly use this issue to cause SQLite to crash, resulting in a denial of service.

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

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

See Also

https://ubuntu.com/security/notices/USN-6566-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0013

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-2023-7104
XREF	IAVA:2024-A-0003
XREF	USN:6566-2

Plugin Information

Published: 2024/06/26, 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 : libsqlite3-0_3.22.0-1ubuntu0.7
  - Fixed package     : libsqlite3-0_3.22.0-1ubuntu0.7+esm1
```

159490 - OpenSSH < 7.8

Synopsis

The SSH server running on the remote host is affected by a information disclosure vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 7.8. It is, therefore, affected by an information disclosure vulnerability in the auth2-gss.c, auth2-hostbased.c, and auth2-pubkey due to not delaying for an invalid authenticating user. An unauthenticated, remote attacker can exploit this, via a malformed packet, to potentially enumerate users.

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

See Also

https://www.openwall.com/lists/oss-security/2018/08/15/5

https://www.openssh.com/txt/release-7.8

Solution

Upgrade to OpenSSH version 7.8 or later.

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

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

VPR Score

4.9

EPSS Score

0.0237

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

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

References

CVE CVE-2018-15473

Exploitable With

CANVAS (true)

Plugin Information

Published: 2022/04/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Installed version : 7.6p1
Fixed version     : 7.8
```

159491 - OpenSSH < 8.0

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is prior to 8.0. It is, therefore, affected by the following vulnerabilities:

- A permission bypass vulnerability due to improper directory name validation. An unauthenticated, remote attacker can exploit this, with a specially crafted scp server, to change the permission of a directory on the client. (CVE-2018-20685)

- Multiple arbitrary file downloads due to improper validation of object name and stderr output. An unauthenticated remote attacker can exploit this, with a specially crafted scp server, to include additional hidden files in the transfer. (CVE-2019-6109, CVE-2019-6110)

- An arbitrary file write vulnerability due to improper object name validation. An unauthenticated, remote attacker can exploit this, with a specially crafted scp server, to overwrite arbitrary files in the client directory. (CVE-2019-6111)

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

See Also

https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

https://www.openssh.com/txt/release-8.0

Solution

Upgrade to OpenSSH version 8.0 or later.

Risk Factor

Medium

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)

VPR Score

6.1

EPSS Score

0.0042

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-2018-20685
CVE	CVE-2019-6109
CVE	CVE-2019-6110
CVE	CVE-2019-6111

Plugin Information

Published: 2022/04/04, Modified: 2024/03/27

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Installed version : 7.6p1
Fixed version     : 8.0
```

187201 - OpenSSH < 9.6 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

The version of OpenSSH installed on the remote host is prior to 9.6. It is, therefore, affected by multiple vulnerabilities as referenced in the release-9.6 advisory.

- ssh(1), sshd(8): implement protocol extensions to thwart the so-called Terrapin attack discovered by Fabian Bumer, Marcus Brinkmann and Jrg Schwenk. This attack allows a MITM to effect a limited break of the integrity of the early encrypted SSH transport protocol by sending extra messages prior to the commencement of encryption, and deleting an equal number of consecutive messages immediately after encryption starts. A peer SSH client/server would not be able to detect that messages were deleted. While cryptographically novel, the security impact of this attack is fortunately very limited as it only allows deletion of consecutive messages, and deleting most messages at this stage of the protocol prevents user user authentication from proceeding and results in a stuck connection. The most serious identified impact is that it lets a MITM to delete the SSH2_MSG_EXT_INFO message sent before authentication starts, allowing the attacker to disable a subset of the keystroke timing obfuscation features introduced in OpenSSH 9.5.

There is no other discernable impact to session secrecy or session integrity. OpenSSH 9.6 addresses this protocol weakness through a new strict KEX protocol extension that will be automatically enabled when both the client and server support it. This extension makes two changes to the SSH transport protocol to improve the integrity of the initial key exchange. Firstly, it requires endpoints to terminate the connection if any unnecessary or unexpected message is received during key exchange (including messages that were previously legal but not strictly required like SSH2_MSG_DEBUG). This removes most malleability from the early protocol. Secondly, it resets the Message Authentication Code counter at the conclusion of each key exchange, preventing previously inserted messages from being able to make persistent changes to the sequence number across completion of a key exchange. Either of these changes should be sufficient to thwart the Terrapin Attack. More details of these changes are in the PROTOCOL file in the OpenSSH source distribition. (CVE-2023-48795)

- ssh-agent(1): when adding PKCS#11-hosted private keys while specifying destination constraints, if the PKCS#11 token returned multiple keys then only the first key had the constraints applied. Use of regular private keys, FIDO tokens and unconstrained keys are unaffected. (CVE-2023-51384)

- ssh(1): if an invalid user or hostname that contained shell metacharacters was passed to ssh(1), and a ProxyCommand, LocalCommand directive or match exec predicate referenced the user or hostname via %u, %h or similar expansion token, then an attacker who could supply arbitrary user/hostnames to ssh(1) could potentially perform command injection depending on what quoting was present in the user-supplied ssh_config(5) directive. This situation could arise in the case of git submodules, where a repository could contain a submodule with shell characters in its user/hostname. Git does not ban shell metacharacters in user or host names when checking out repositories from untrusted sources. Although we believe it is the user's responsibility to ensure validity of arguments passed to ssh(1), especially across a security boundary such as the git example above, OpenSSH 9.6 now bans most shell metacharacters from user and hostnames supplied via the command-line. This countermeasure is not guaranteed to be effective in all situations, as it is infeasible for ssh(1) to universally filter shell metacharacters potentially relevant to user-supplied commands. User/hostnames provided via ssh_config(5) are not subject to these restrictions, allowing configurations that use strange names to continue to be used, under the assumption that the user knows what they are doing in their own configuration files. (CVE-2023-51385)

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

See Also

https://www.openssh.com/txt/release-9.6

Solution

Upgrade to OpenSSH version 9.6 or later.

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)

VPR Score

6.1

EPSS Score

0.9647

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-2023-51384
CVE	CVE-2023-51385
XREF	IAVA:2023-A-0701-S

Plugin Information

Published: 2023/12/22, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Version source    : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
Installed version : 7.6p1
Fixed version     : 9.6p1 / 9.6
```

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)

VPR Score

6.1

EPSS Score

0.9647

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha1-etm@openssh.com
```

200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a

denial of service, or possibly execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-6827-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0004

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm6
```

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)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28219
XREF	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_5.1.0-1ubuntu0.8
  - Fixed package     : python3-pil_5.1.0-1ubuntu0.8+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0004

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-2023-4641
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_1:4.5-1ubuntu2.5
  - Fixed package     : login_1:4.5-1ubuntu2.5+esm1

  - Installed package : passwd_1:4.5-1ubuntu2.5
  - Fixed package     : passwd_1:4.5-1ubuntu2.5+esm1
```

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)

VPR Score

4.2

EPSS Score

0.0004

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-common_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-common_2:8.0.1453-1ubuntu1.13+esm9

  - Installed package : vim-tiny_2:8.0.1453-1ubuntu1.13
  - Fixed package     : vim-tiny_2:8.0.1453-1ubuntu1.13+esm9

  - Installed package : xxd_2:8.0.1453-1ubuntu1.13
  - Fixed package     : xxd_2:8.0.1453-1ubuntu1.13+esm9
```

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.

Original advisory details:

Matthias Gerstner discovered that the PAM pam_namespace module incorrectly

handled special files when performing directory checks. A local attacker

could possibly use this issue to cause PAM to stop responding, resulting in

a denial of service.

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

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

See Also

https://ubuntu.com/security/notices/USN-6588-2

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)

VPR Score

4.4

EPSS Score

0.0004

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: 2024/08/27

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_1.1.8-3.6ubuntu2.18.04.6
  - Fixed package     : libpam-modules_1.1.8-3.6ubuntu2.18.04.6+esm1

  - Installed package : libpam-modules-bin_1.1.8-3.6ubuntu2.18.04.6
  - Fixed package     : libpam-modules-bin_1.1.8-3.6ubuntu2.18.04.6+esm1

  - Installed package : libpam-runtime_1.1.8-3.6ubuntu2.18.04.6
  - Fixed package     : libpam-runtime_1.1.8-3.6ubuntu2.18.04.6+esm1

  - Installed package : libpam0g_1.1.8-3.6ubuntu2.18.04.6
  - Fixed package     : libpam0g_1.1.8-3.6ubuntu2.18.04.6+esm1
```

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.

Original advisory details:

Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

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

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

See Also

https://ubuntu.com/security/notices/USN-6944-2

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)

VPR Score

4.4

EPSS Score

0.0006

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
XREF	IAVA:2024-A-0457-S

Plugin Information

Published: 2024/08/21, Modified: 2024/09/13

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 : libcurl3-gnutls_7.58.0-2ubuntu3.24
  - Fixed package     : libcurl3-gnutls_7.58.0-2ubuntu3.24+esm5
```

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)

VPR Score

3.6

EPSS Score

0.0005

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_6.1-1ubuntu1.18.04.1
  - Fixed package     : libncurses5_6.1-1ubuntu1.18.04.1+esm2

  - Installed package : libncursesw5_6.1-1ubuntu1.18.04.1
  - Fixed package     : libncursesw5_6.1-1ubuntu1.18.04.1+esm2

  - Installed package : libtinfo5_6.1-1ubuntu1.18.04.1
  - Fixed package     : libtinfo5_6.1-1ubuntu1.18.04.1+esm2

  - Installed package : ncurses-base_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-base_6.1-1ubuntu1.18.04.1+esm2

  - Installed package : ncurses-bin_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-bin_6.1-1ubuntu1.18.04.1+esm2

  - Installed package : ncurses-term_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-term_6.1-1ubuntu1.18.04.1+esm2
```

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)

VPR Score

4.4

EPSS Score

0.0004

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_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick_8:6.9.7.4+dfsg-16ubuntu6.15+esm3

  - Installed package : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6-common_8:6.9.7.4+dfsg-16ubuntu6.15+esm3

  - Installed package : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : imagemagick-6.q16_8:6.9.7.4+dfsg-16ubuntu6.15+esm3

  - Installed package : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm3

  - Installed package : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-16ubuntu6.15+esm3

  - Installed package : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15
  - Fixed package     : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-16ubuntu6.15+esm3
```

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)

VPR Score

3.6

EPSS Score

0.0004

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_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-autoipd_0.7-3.1ubuntu1.3+esm2

  - Installed package : avahi-daemon_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-daemon_0.7-3.1ubuntu1.3+esm2

  - Installed package : avahi-utils_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-utils_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-client3_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-client3_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-common-data_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-common-data_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-common3_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-common3_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-core7_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-core7_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-glib1_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-glib1_0.7-3.1ubuntu1.3+esm2

  - Installed package : libavahi-ui-gtk3-0_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-ui-gtk3-0_0.7-3.1ubuntu1.3+esm2
```

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)

VPR Score

6.5

EPSS Score

0.0008

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_5.48-0ubuntu3.9
  - Fixed package     : bluez_5.48-0ubuntu3.9+esm1

  - Installed package : bluez-cups_5.48-0ubuntu3.9
  - Fixed package     : bluez-cups_5.48-0ubuntu3.9+esm1

  - Installed package : bluez-obexd_5.48-0ubuntu3.9
  - Fixed package     : bluez-obexd_5.48-0ubuntu3.9+esm1

  - Installed package : libbluetooth3_5.48-0ubuntu3.9
  - Fixed package     : libbluetooth3_5.48-0ubuntu3.9+esm1
```

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/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0008

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_3.20191021.1+really3.20181128.1~ubuntu0.18.04.1
  - Fixed package     : amd64-microcode_3.20191021.1+really3.20181128.1~ubuntu0.18.04.1+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)

VPR Score

6.1

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-20569
XREF	USN:6319-1

Plugin Information

Published: 2023/08/30, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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_3.20191021.1+really3.20181128.1~ubuntu0.18.04.1
  - Fixed package     : amd64-microcode_3.20191021.1+really3.20181128.1~ubuntu0.18.04.1+esm2
```

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)

VPR Score

4.4

EPSS Score

0.0007

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+0-0ubuntu0.18.04.18
  - Fixed package     : ghostscript_9.26~dfsg+0-0ubuntu0.18.04.18+esm1

  - Installed package : ghostscript-x_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : ghostscript-x_9.26~dfsg+0-0ubuntu0.18.04.18+esm1

  - Installed package : libgs9_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : libgs9_9.26~dfsg+0-0ubuntu0.18.04.18+esm1

  - Installed package : libgs9-common_9.26~dfsg+0-0ubuntu0.18.04.18
  - Fixed package     : libgs9-common_9.26~dfsg+0-0ubuntu0.18.04.18+esm1
```

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 to 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)

VPR Score

7.4

EPSS Score

0.0008

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_3.20230214.0ubuntu0.18.04.1
  - Fixed package     : intel-microcode_3.20230808.0ubuntu0.18.04.1+esm1
```

179893 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerabilities (USN-6290-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6290-1 advisory.

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files with the tiffcrop utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-48281)

It was discovered that LibTIFF incorrectly handled certain image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04. (CVE-2023-2731)

It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-2908)

It was discovered that LibTIFF incorrectly handled certain file paths. If a user were tricked into specifying certain output paths, an attacker could possibly use this issue to cause a denial of service.

This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-3316)

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2023-3618)

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-25433, CVE-2023-26966)

It was discovered that LibTIFF did not properly managed memory when processing certain malformed image files with the tiffcrop utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-26965)

It was discovered that LibTIFF contained an arithmetic overflow. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service.

(CVE-2023-38288, CVE-2023-38289)

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

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

See Also

https://ubuntu.com/security/notices/USN-6290-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0024

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm2
```

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)

VPR Score

5.0

EPSS Score

0.0005

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm3
```

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)

VPR Score

4.4

EPSS Score

0.0006

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+esm4
```

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)

VPR Score

4.4

EPSS Score

0.0081

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 : libdw1_0.170-0.4ubuntu0.1
  - Fixed package     : libdw1_0.170-0.4ubuntu0.1+esm1

  - Installed package : libelf1_0.170-0.4ubuntu0.1
  - Fixed package     : libelf1_0.170-0.4ubuntu0.1+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0012

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_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler-glib8_0.62.0-2ubuntu2.14+esm1

  - Installed package : libpoppler73_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler73_0.62.0-2ubuntu2.14+esm1

  - Installed package : poppler-utils_0.62.0-2ubuntu2.14
  - Fixed package     : poppler-utils_0.62.0-2ubuntu2.14+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.

Original advisory details:

It was discovered that Avahi incorrectly handled certain DBus messages. A

local attacker could possibly use this issue to cause Avahi to crash,

resulting in a denial of service.

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

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

See Also

https://ubuntu.com/security/notices/USN-6129-2

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)

VPR Score

4.4

EPSS Score

0.0004

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: 2024/08/27

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_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-autoipd_0.7-3.1ubuntu1.3+esm1

  - Installed package : avahi-daemon_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-daemon_0.7-3.1ubuntu1.3+esm1

  - Installed package : avahi-utils_0.7-3.1ubuntu1.3
  - Fixed package     : avahi-utils_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-client3_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-client3_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-common-data_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-common-data_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-common3_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-common3_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-core7_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-core7_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-glib1_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-glib1_0.7-3.1ubuntu1.3+esm1

  - Installed package : libavahi-ui-gtk3-0_0.7-3.1ubuntu1.3
  - Fixed package     : libavahi-ui-gtk3-0_0.7-3.1ubuntu1.3+esm1
```

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.

Original advisory details:

It was discovered that CUPS incorrectly authenticated certain remote

requests. A remote attacker could possibly use this issue to obtain

recently printed documents.

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

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

See Also

https://ubuntu.com/security/notices/USN-6361-2

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)

VPR Score

4.4

EPSS Score

0.0004

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: 2024/08/28

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 : cups_2.2.7-1ubuntu2.10
  - Fixed package     : cups_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-bsd_2.2.7-1ubuntu2.10
  - Fixed package     : cups-bsd_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-client_2.2.7-1ubuntu2.10
  - Fixed package     : cups-client_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-common_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-core-drivers_2.2.7-1ubuntu2.10
  - Fixed package     : cups-core-drivers_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-daemon_2.2.7-1ubuntu2.10
  - Fixed package     : cups-daemon_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-ipp-utils_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ipp-utils_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-ppdc_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ppdc_2.2.7-1ubuntu2.10+esm3

  - Installed package : cups-server-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-server-common_2.2.7-1ubuntu2.10+esm3

  - Installed package : libcups2_2.2.7-1ubuntu2.10
  - Fixed package     : libcups2_2.2.7-1ubuntu2.10+esm3
```

```
  - Installed package : libcupscgi1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupscgi1_2.2.7-1ubuntu2.10+esm3

  - Installed package : libcupsimage2_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsimage2_2.2.7-1ubuntu2.10+esm3

  - Installed package : libcupsmime1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsmime1_2.2.7-1ubuntu2.10+esm3

  - Installed package : libcupsppdc1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsppdc1_2.2.7-1ubuntu2.10+esm3
```

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 kadmind, which could lead to the freeing of uninitialized memory. An authenticated remote attacker could possibly use this issue to cause kadmind 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/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0043

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

tcp/0

```
NOTE: This vulnerability check contains 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_1.16-2ubuntu0.4
  - Fixed package     : krb5-locales_1.16-2ubuntu0.4+esm1

  - Installed package : libgssapi-krb5-2_1.16-2ubuntu0.4
  - Fixed package     : libgssapi-krb5-2_1.16-2ubuntu0.4+esm1

  - Installed package : libk5crypto3_1.16-2ubuntu0.4
  - Fixed package     : libk5crypto3_1.16-2ubuntu0.4+esm1

  - Installed package : libkrb5-3_1.16-2ubuntu0.4
  - Fixed package     : libkrb5-3_1.16-2ubuntu0.4+esm1

  - Installed package : libkrb5support0_1.16-2ubuntu0.4
  - Fixed package     : libkrb5support0_1.16-2ubuntu0.4+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0009

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_4.0.9-5ubuntu0.10
  - Fixed package     : libtiff5_4.0.9-5ubuntu0.10+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.

Original advisory details:

Fabian Bumer, Marcus Brinkmann, Jrg Schwenk discovered that the SSH

protocol was vulnerable to a prefix truncation attack. If a remote attacker

was able to intercept SSH communications, extension negotiation messages

could be truncated, possibly leading to certain algorithms and features

being downgraded. This issue is known as the Terrapin attack. This update

adds protocol extensions to mitigate this issue. (CVE-2023-48795)

It was discovered that OpenSSH incorrectly handled user names or host names

with shell metacharacters. An attacker could possibly use this issue to

perform OS command injection. This only affected Ubuntu 18.04 LTS. (CVE-2023-51385)

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

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

See Also

https://ubuntu.com/security/notices/USN-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)

VPR Score

6.1

EPSS Score

0.9647

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: 2024/09/18

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 : openssh-client_1:7.6p1-4ubuntu0.7
```

```
  - Fixed package     : openssh-client_1:7.6p1-4ubuntu0.7+esm3

  - Installed package : openssh-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-server_1:7.6p1-4ubuntu0.7+esm3

  - Installed package : openssh-sftp-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-sftp-server_1:7.6p1-4ubuntu0.7+esm3
```

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0052

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 : libssl1.1_1.1.1-1ubuntu2.1~18.04.23
  - Fixed package     : libssl1.1_1.1.1-1ubuntu2.1~18.04.23+esm3

  - Installed package : openssl_1.1.1-1ubuntu2.1~18.04.23
  - Fixed package     : openssl_1.1.1-1ubuntu2.1~18.04.23+esm3
```

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0008

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_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13+esm4

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13+esm4

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13+esm4

  - Installed package : libpython3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6_3.6.9-1~18.04ubuntu1.13+esm1

  - Installed package : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-minimal_3.6.9-1~18.04ubuntu1.13+esm1

  - Installed package : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : libpython3.6-stdlib_3.6.9-1~18.04ubuntu1.13+esm1

  - Installed package : python3.6_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6_3.6.9-1~18.04ubuntu1.13+esm1

  - Installed package : python3.6-minimal_3.6.9-1~18.04ubuntu1.12
  - Fixed package     : python3.6-minimal_3.6.9-1~18.04ubuntu1.13+esm1
```

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)

VPR Score

4.4

EPSS Score

0.0012

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-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_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7_2.7.17-1~18.04ubuntu1.13+esm2

  - Installed package : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-minimal_2.7.17-1~18.04ubuntu1.13+esm2

  - Installed package : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.11
  - Fixed package     : libpython2.7-stdlib_2.7.17-1~18.04ubuntu1.13+esm2
```

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.

Original advisory details:

Dennis Brinkrolf and Tobias Funke discovered that Requests incorrectly

leaked Proxy-Authorization headers. A remote attacker could possibly use

this issue to obtain sensitive information.

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

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

See Also

https://ubuntu.com/security/notices/USN-6155-2

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0027

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: 2024/09/19

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-requests_2.18.4-2ubuntu0.1
  - Fixed package     : python3-requests_2.18.4-2ubuntu0.1+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.

Original advisory details:

Hiroki Kurosawa discovered that curl incorrectly handled validating certain

certificate wildcards. A remote attacker could possibly use this issue to

spoof certain website certificates using IDN hosts. (CVE-2023-28321)

Hiroki Kurosawa discovered that curl incorrectly handled callbacks when

certain options are set by applications. This could cause applications

using curl to misbehave, resulting in information disclosure, or a denial

of service. (CVE-2023-28322)

It was discovered that curl incorrectly handled saving cookies to files. A

local attacker could possibly use this issue to create or overwrite files.

This issue only affected Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-32001)

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

Note that Nessus has not tested 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)

VPR Score

4.4

EPSS Score

0.0019

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: 2024/08/27

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-gnutls_7.58.0-2ubuntu3.24
  - Fixed package     : libcurl3-gnutls_7.58.0-2ubuntu3.24+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.

Original advisory details:

It was discovered that libssh incorrectly handled the ProxyCommand and the

ProxyJump features. A remote attacker could possibly use this issue to

inject malicious code into the command of the features mentioned through

the hostname parameter. (CVE-2023-6004)

It was discovered that libssh incorrectly handled return codes when

performing message digest operations. A remote attacker could possibly use

this issue to cause libssh to crash, obtain sensitive information, or

execute arbitrary code. (CVE-2023-6918)

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

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

See Also

https://ubuntu.com/security/notices/USN-6592-2

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)

VPR Score

4.2

EPSS Score

0.0006

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: 2024/08/28

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 : libssh-4_0.8.0~20170825.94fa1e38-1ubuntu0.7
  - Fixed package     : libssh-4_0.8.0~20170825.94fa1e38-1ubuntu0.7+esm3
```

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

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0044

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-19189
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_6.1-1ubuntu1.18.04.1
  - Fixed package     : libncurses5_6.1-1ubuntu1.18.04.1+esm1

  - Installed package : libncursesw5_6.1-1ubuntu1.18.04.1
  - Fixed package     : libncursesw5_6.1-1ubuntu1.18.04.1+esm1

  - Installed package : libtinfo5_6.1-1ubuntu1.18.04.1
  - Fixed package     : libtinfo5_6.1-1ubuntu1.18.04.1+esm1

  - Installed package : ncurses-base_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-base_6.1-1ubuntu1.18.04.1+esm1

  - Installed package : ncurses-bin_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-bin_6.1-1ubuntu1.18.04.1+esm1

  - Installed package : ncurses-term_6.1-1ubuntu1.18.04.1
  - Fixed package     : ncurses-term_6.1-1ubuntu1.18.04.1+esm1
```

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)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-21123
CVE	CVE-2022-21125
CVE	CVE-2022-21166
XREF	USN:5485-1

Plugin Information

Published: 2022/06/17, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-120-generic
 for this advisory.
```

200879 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : CUPS vulnerability (USN-6844-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6844-1 advisory.

Rory McNamara discovered that when starting the cupsd server with a Listen configuration item, the cupsd process fails to validate if bind call passed. An attacker could possibly trick cupsd to perform an arbitrary chmod of the provided argument, providing world-writable access to the target.

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

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

See Also

https://ubuntu.com/security/notices/USN-6844-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0004

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_2.2.7-1ubuntu2.10
  - Fixed package     : cups_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-bsd_2.2.7-1ubuntu2.10
  - Fixed package     : cups-bsd_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-client_2.2.7-1ubuntu2.10
  - Fixed package     : cups-client_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-common_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-core-drivers_2.2.7-1ubuntu2.10
  - Fixed package     : cups-core-drivers_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-daemon_2.2.7-1ubuntu2.10
  - Fixed package     : cups-daemon_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-ipp-utils_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ipp-utils_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-ppdc_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ppdc_2.2.7-1ubuntu2.10+esm4

  - Installed package : cups-server-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-server-common_2.2.7-1ubuntu2.10+esm4

  - Installed package : libcups2_2.2.7-1ubuntu2.10
  - Fixed package     : libcups2_2.2.7-1ubuntu2.10+esm4

  - Installed package : libcupscgi1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupscgi1_2.2.7-1ubuntu2.10+esm4

  - Installed package : libcupsimage2_2.2.7-1ubuntu2.10
```

```
  - Fixed package     : libcupsimage2_2.2.7-1ubuntu2.10+esm4

  - Installed package : libcupsmime1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsmime1_2.2.7-1ubuntu2.10+esm4

  - Installed package : libcupsppdc1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsppdc1_2.2.7-1ubuntu2.10+esm4
```

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

Medium

CVSS v3.0 Base Score

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

VPR Score

6.7

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.1 (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: 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_5.48-0ubuntu3.9
  - Fixed package     : bluez_5.48-0ubuntu3.9+esm2

  - Installed package : bluez-cups_5.48-0ubuntu3.9
  - Fixed package     : bluez-cups_5.48-0ubuntu3.9+esm2

  - Installed package : bluez-obexd_5.48-0ubuntu3.9
  - Fixed package     : bluez-obexd_5.48-0ubuntu3.9+esm2

  - Installed package : libbluetooth3_5.48-0ubuntu3.9
  - Fixed package     : libbluetooth3_5.48-0ubuntu3.9+esm2
```

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)

VPR Score

4.4

EPSS Score

0.0008

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_8.1.1-0ubuntu1
  - Fixed package     : gdb_8.1.1-0ubuntu1+esm1

  - Installed package : gdbserver_8.1.1-0ubuntu1
  - Fixed package     : gdbserver_8.1.1-0ubuntu1+esm1
```

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)

Bahaa 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)

VPR Score

4.4

EPSS Score

0.0023

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 : libssl1.1_1.1.1-1ubuntu2.1~18.04.23
  - Fixed package     : libssl1.1_1.1.1-1ubuntu2.1~18.04.23+esm4

  - Installed package : openssl_1.1.1-1ubuntu2.1~18.04.23
  - Fixed package     : openssl_1.1.1-1ubuntu2.1~18.04.23+esm4
```

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/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)

VPR Score

3.3

EPSS Score

0.0007

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-gnutls_7.58.0-2ubuntu3.24
  - Fixed package     : libcurl3-gnutls_7.58.0-2ubuntu3.24+esm3
```

182578 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6417-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6417-1 advisory.

It was discovered that the eBPF implementation in the Linux kernel contained a race condition around read- only maps. A privileged attacker could use this to modify read-only maps. (CVE-2021-4001)

It was discovered that the IPv6 implementation in the Linux kernel contained a high rate of hash collisions in connection lookup table. A remote attacker could use this to cause a denial of service (excessive CPU consumption). (CVE-2023-1206)

Yang Lan discovered that the GFS2 file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious GFS2 image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2023-3212)

Davide Ornaghi discovered that the DECnet network protocol implementation in the Linux kernel contained a null pointer dereference vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. Please note that kernel support for the DECnet has been removed to resolve this CVE. (CVE-2023-3338)

It was discovered that the NFC implementation in the Linux kernel contained a use-after-free vulnerability when performing peer-to-peer communication in certain conditions. A privileged attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory).

(CVE-2023-3863)

It was discovered that the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-4194)

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

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

See Also

https://ubuntu.com/security/notices/USN-6417-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0069

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-4001
CVE	CVE-2023-1206
CVE	CVE-2023-3212
CVE	CVE-2023-3338
CVE	CVE-2023-3863
CVE	CVE-2023-4194
XREF	USN:6417-1

Plugin Information

Published: 2023/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-164-generic
 for this advisory.
```

184085 - Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6462-1)

Synopsis

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

Description

The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6462-1 advisory.

Seth Jenkins discovered that the Linux kernel did not properly perform address randomization for a per-cpu memory management structure. A local attacker could use this to expose sensitive information (kernel memory) or in conjunction with another kernel vulnerability. (CVE-2023-0597)

Yu Hao and Weiteng Chen discovered that the Bluetooth HCI UART driver in the Linux kernel contained a race condition, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-31083)

Lin Ma discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a null pointer dereference vulnerability in some situations. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-3772)

It was discovered that the Siano USB MDTV receiver device driver in the Linux kernel did not properly handle device initialization failures in certain situations, leading to a use-after-free vulnerability. A physically proximate attacker could use this cause a denial of service (system crash). (CVE-2023-4132)

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

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

See Also

https://ubuntu.com/security/notices/USN-6462-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-0597
CVE	CVE-2023-3772
CVE	CVE-2023-4132
CVE	CVE-2023-31083
XREF	USN:6462-1

Plugin Information

Published: 2023/10/31, Modified: 2024/08/28

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-166-generic
 for this advisory.
```

187680 - Ubuntu 18.04 ESM : GnuTLS vulnerability (USN-6499-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6499-2 advisory.

USN-6499-1 fixed vulnerabilities in GnuTLS. This update provides the corresponding update for Ubuntu 18.04 LTS.

Original advisory details:

It was discovered that GnuTLS had a timing side-channel when handling

certain RSA-PSK key exchanges. A remote attacker could possibly use this

issue to recover sensitive information.

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

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

See Also

https://ubuntu.com/security/notices/USN-6499-2

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

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)

VPR Score

4.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5981
XREF	USN:6499-2

Plugin Information

Published: 2024/01/08, 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 : libgnutls30_3.5.18-1ubuntu1.6
  - Fixed package     : libgnutls30_3.5.18-1ubuntu1.6+esm1
```

201188 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : eSpeak NG vulnerabilities (USN-6858-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6858-1 advisory.

It was discovered that eSpeak NG did not properly manage memory under certain circumstances. An attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2023-49990, CVE-2023-49991, CVE-2023-49992, CVE-2023-49993, CVE-2023-49994)

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

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

See Also

https://ubuntu.com/security/notices/USN-6858-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0006

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-49990
CVE	CVE-2023-49991
CVE	CVE-2023-49992
CVE	CVE-2023-49993
CVE	CVE-2023-49994
XREF	USN:6858-1

Plugin Information

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

Plugin Output

tcp/0

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


  - Installed package : espeak-ng-data_1.49.2+dfsg-1
  - Fixed package     : espeak-ng-data_1.49.2+dfsg-1ubuntu0.1~esm1

  - Installed package : libespeak-ng1_1.49.2+dfsg-1
  - Fixed package     : libespeak-ng1_1.49.2+dfsg-1ubuntu0.1~esm1
```

162689 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel (HWE) vulnerability (USN-5493-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5493-2 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-5493-2

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)

VPR Score

3.6

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-28388
XREF	USN:5493-2

Plugin Information

Published: 2022/07/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-121-generic
 for this advisory.
```

155749 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5163-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5163-1 advisory.

Ilja Van Sprundel discovered that the SCTP implementation in the Linux kernel did not properly perform size validations on incoming packets in some situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2021-3655)

It was discovered that the Option USB High Speed Mobile device driver in the Linux kernel did not properly handle error conditions. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-37159)

It was discovered that the AMD Cryptographic Coprocessor (CCP) driver in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3744, CVE-2021-3764)

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

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

See Also

https://ubuntu.com/security/notices/USN-5163-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3655
CVE	CVE-2021-3744
CVE	CVE-2021-3764
CVE	CVE-2021-37159
XREF	USN:5163-1

Plugin Information

Published: 2021/12/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-91-generic
 for this advisory.
```

163113 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5514-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5514-1 advisory.

It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1195)

Duoming Zhou discovered that the AX.25 amateur radio protocol implementation in the Linux kernel did not handle detach events properly in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1199)

Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel during device detach operations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1204)

Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel, leading to use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1205)

Yongkang Jia discovered that the KVM hypervisor implementation in the Linux kernel did not properly handle guest TLB mapping invalidation requests in some situations. An attacker in a guest VM could use this to cause a denial of service (system crash) in the host OS. (CVE-2022-1789)

Minh Yuan discovered that the floppy driver in the Linux kernel contained a race condition in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-33981)

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

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

See Also

https://ubuntu.com/security/notices/USN-5514-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0027

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-2022-1195
CVE	CVE-2022-1199
CVE	CVE-2022-1204
CVE	CVE-2022-1205
CVE	CVE-2022-1789
CVE	CVE-2022-33981
XREF	USN:5514-1

Plugin Information

Published: 2022/07/14, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-122-generic
 for this advisory.
```

197218 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6776-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6776-1 advisory.

Zheng Wang discovered that the Broadcom FullMAC WLAN driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-47233)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Networking core;

- IPv4 networking;

- MAC80211 subsystem;

- Tomoyo security module; (CVE-2024-26614, CVE-2023-52530, CVE-2024-26622)

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

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

See Also

https://ubuntu.com/security/notices/USN-6776-1

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0004

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-2023-47233
CVE	CVE-2023-52530
CVE	CVE-2024-26614
CVE	CVE-2024-26622
XREF	USN:6776-1

Plugin Information

Published: 2024/05/16, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-182-generic
 for this advisory.
```

164681 - Ubuntu 18.04 LTS : Linux kernel (HWE) vulnerabilities (USN-5600-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5600-1 advisory.

Asaf Modelevsky discovered that the Intel(R) 10GbE PCI Express (ixgbe) Ethernet driver for the Linux kernel performed insufficient control flow management. A local attacker could possibly use this to cause a denial of service. (CVE-2021-33061)

It was discovered that the virtual terminal driver in the Linux kernel did not properly handle VGA console font changes, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33656)

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

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

See Also

https://ubuntu.com/security/notices/USN-5600-1

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-33061
CVE	CVE-2021-33656
XREF	USN:5600-1

Plugin Information

Published: 2022/09/05, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-125-generic
 for this advisory.
```

192404 - Ubuntu 18.04 LTS : OpenSSL vulnerabilities (USN-6709-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6709-1 advisory.

It was discovered that checking excessively long DH keys or parameters may be very slow. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, resulting in a denial of service.

(CVE-2023-3446)

After the fix for CVE-2023-3446 Bernd Edlinger discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, resulting in a denial of service. (CVE-2023-3817)

David Benjamin discovered that generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, resulting in a denial of service. (CVE-2023-5678)

Bahaa Naamneh discovered that processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack. (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-6709-1

Solution

Update the affected libssl1.0-dev, libssl1.0.0 and / or openssl1.0 packages.

Risk Factor

Medium

CVSS v4.0 Base Score

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

CVSS v3.0 Base Score

5.5 (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)

VPR Score

4.4

EPSS Score

0.0052

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-3446
CVE	CVE-2023-3817
CVE	CVE-2023-5678
CVE	CVE-2024-0727
XREF	USN:6709-1

Plugin Information

Published: 2024/03/21, 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_1.0.2n-1ubuntu5.13
  - Fixed package     : libssl1.0.0_1.0.2n-1ubuntu5.13+esm1
```

200807 - urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891)

Synopsis

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

Description

urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with 'ProxyManager', the 'Proxy-Authorization' header is only sent to the configured proxy, as expected. However, when sending HTTP requests without using urllib3's proxy support, it's possible to accidentally configure the 'Proxy-Authorization' header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the 'Proxy-Authorization' HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects.

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

See Also

http://www.nessus.org/u?7b44847c

Solution

Upgrade to urllib3 version 1.26.19, 2.2.2 or later.

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)

VPR Score

3.6

EPSS Score

0.0004

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)

STIG Severity

II

References

CVE	CVE-2024-37891
XREF	IAVA:2024-A-0363

Plugin Information

Published: 2024/06/21, Modified: 2024/09/18

Plugin Output

tcp/0

```
Installed version : 1.22
Fixed version     : 1.26.19
```

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

VPR Score

4.2

EPSS Score

0.8808

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: 2024/09/04

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

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

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)

VPR Score

1.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-39804
XREF	USN:6543-1

Plugin Information

Published: 2023/12/11, Modified: 2024/08/27

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_1.29b-2ubuntu0.4
  - Fixed package     : tar_1.29b-2ubuntu0.4+esm1
```

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)

VPR Score

1.4

EPSS Score

0.0004

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 : libprocps6_2:3.3.12-3ubuntu1.2
  - Fixed package     : libprocps6_2:3.3.12-3ubuntu1.2+esm1

  - Installed package : procps_2:3.3.12-3ubuntu1.2
  - Fixed package     : procps_2:3.3.12-3ubuntu1.2+esm1
```

178940 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Open VM Tools vulnerability (USN-6257-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6257-1 advisory.

It was discovered that Open VM Tools incorrectly handled certain authentication requests. A fully compromised ESXi host can force Open VM Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. (CVE-2023-20867)

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

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

See Also

https://ubuntu.com/security/notices/USN-6257-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.6

EPSS Score

0.0031

CVSS v2.0 Base Score

2.3 (CVSS2#AV:L/AC:H/Au:M/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-20867
XREF	USN:6257-1
XREF	CISA-KNOWN-EXPLOITED:2023/07/14

Plugin Information

Published: 2023/07/27, Modified: 2024/08/28

Plugin Output

tcp/0

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


  - Installed package : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools_2:11.0.5-4ubuntu0.18.04.3+esm1

  - Installed package : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3
  - Fixed package     : open-vm-tools-desktop_2:11.0.5-4ubuntu0.18.04.3+esm1
```

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.

Original advisory details:

It was discovered that curl incorrectly handled cookies when an application

duplicated certain handles. A local attacker could possibly create a cookie

file and inject arbitrary cookies into subsequent connections.

(CVE-2023-38546)

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

Note that Nessus has not tested for 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)

VPR Score

2.2

EPSS Score

0.0009

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	CVE-2023-38546
XREF	USN:6429-2
XREF	CEA-ID:CEA-2023-0052
XREF	IAVA:2023-A-0531-S

Plugin Information

Published: 2023/10/11, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains 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-gnutls_7.58.0-2ubuntu3.24
  - Fixed package     : libcurl3-gnutls_7.58.0-2ubuntu3.24+esm2
```

160025 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5384-1)

Synopsis

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

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5384-1 advisory.

It was discovered that the UDF file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious UDF image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2022-0617)

Lyu Tao discovered that the NFS implementation in the Linux kernel did not properly handle requests to open a directory on a regular file. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-24448)

It was discovered that the YAM AX.25 device driver in the Linux kernel did not properly deallocate memory in some error conditions. A local privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2022-24959)

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

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

See Also

https://ubuntu.com/security/notices/USN-5384-1

Solution

Update the affected kernel package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0617
CVE	CVE-2022-24448
CVE	CVE-2022-24959
XREF	USN:5384-1

Plugin Information

Published: 2022/04/21, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-109-generic
 for this advisory.
```

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      : None
Vendor       : VMware, Inc.
Release Date : 11/12/2020
Secure boot  : disabled
```

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: 2024/09/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:18.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:exiv2:libexiv2:0.25
  cpe:/a:gnome:gnome-shell:3.28.4 -> GNOME gnome-shell -
  cpe:/a:gnupg:libgcrypt:1.8.1 -> GnuPG Libgcrypt
  cpe:/a:haxx:libcurl:7.58.0 -> Haxx libcurl
  cpe:/a:openbsd:openssh:7.6 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:7.6p1 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1 -> OpenSSL Project OpenSSL
  cpe:/a:tukaani:xz:5.2.2 -> Tukaani XZ
  cpe:/a:vim:vim:8.0 -> Vim
  cpe:/a:vmware:open_vm_tools:11.0.5 -> VMware Open VM Tools
```

```
x-cpe:/a:libndp:libndp:1.6
```

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: 2024/09/03

Plugin Output

tcp/0

```
Hostname : osboxes
  osboxes (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: 2022/09/09

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: 2024/02/05

Plugin Output

tcp/0

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

 - 127.0.0.1 (on interface lo)
 - 192.168.217.130 (on interface ens33)
```

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: 2022/02/23

Plugin Output

tcp/0

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

 - ::1 (on interface lo)
 - fe80::4667:1a40:bad5:bd1c (on interface ens33)
```

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 :

  - 00:0c:29:09:9c:d7 (interface ens33)
```

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: 2023/11/17

Plugin Output

tcp/0

```
ens33:
  MAC : 00:0c:29:09:9c:d7
  IPv4:
    - Address : 192.168.217.130
      Netmask : 255.255.255.0
      Broadcast : 192.168.217.255
  IPv6:
    - Address : fe80::4667:1a40:bad5:bd1c
      Prefixlen : 64
      Scope : link
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  ens33:
    ipv4_gateways:
      192.168.217.2:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  ens33:
    ipv4_subnets:
     - 169.254.0.0/16
     - 192.168.217.0/24
    ipv6_subnets:
     - fe80::/64
     - fe80::/64
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:09:9C:D7 : VMware, Inc.
```

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: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:09:9C:D7
```

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: 2024/09/11

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ ens33
  + IPv4
    - Address       : 192.168.217.130
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::4667:1a40:bad5:bd1c
      Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2024/09/11

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.2.1
  Version : 1.8.1

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.1
```

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.182774' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://github.com/jpirko/libndp

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2024/09/11

Plugin Output

tcp/0

```
Path          : libndp0 1.6-1 (via package manager)
Version       : 1.6
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            1.9G     0  1.9G   0% /dev
tmpfs           391M  1.9M  389M   1% /run
/dev/sda1       217G  5.8G  200G   3% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop0      640K  640K     0 100% /snap/gnome-logs/106
/dev/loop1       33M   33M     0 100% /snap/snapd/12883
/dev/loop3      768K  768K     0 100% /snap/gnome-characters/726
/dev/loop4      242M  242M     0 100% /snap/gnome-3-38-2004/70
/dev/loop5      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop6      2.5M  2.5M     0 100% /snap/gnome-calculator/884
/dev/loop7       62M   62M     0 100% /snap/core20/1081
/dev/loop8       56M   56M     0 100% /snap/core18/2128
/dev/loop9      2.5M  2.5M     0 100% /snap/gnome-system-monitor/163
/dev/sda3       265G   67M  252G   1% /home
tmpfs           391M   16K  391M   1% /run/user/121
tmpfs           391M   36K  391M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
```

```
loop0    7:0    0   548K  1 loop /snap/gnome-logs/106
loop1    7:1    0  32.3M  1 loop /snap/snapd/12883
loop2    7:2    0  65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   704K  1 loop /snap/gnome-characters/726
loop4    7:4    0 241.4M  1 loop /snap/gnome-3-38-2004/70
loop5    7:5    0   219M  1 loop /snap/gnome-3-34-1804/72
loop6    7:6    0   2.5M  1 loop /snap/gnome-calculator/884
loop7    7:7    0  61.8M  1 loop /snap/core20/1081
loop8    7:8    0  55.4M  1 loop /snap/core18/2128
loop9    7:9    0   2.5M  1 loop /snap/gnome-system-monitor/163
sda      8:0    0   500G  0 disk
├─sda1   8:1    0 220.6G  0 part /
├─sda2   8:2    0   9.3G  0 part [SWAP]
└─sda3   8:3    0 270.1G  0 part /home
sr0     11:0    1  1024M  0 rom


$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
ude [...]
```

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: 2024/03/13

Plugin Output

tcp/0

```
-----------[ User Accounts ]-----------

User         : osboxes
Home folder  : /home/osboxes
Start script : /bin/bash
Groups       : osboxes
               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
Home folder  : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups       : uucp

User         : proxy
Home folder  : /bin
Start script : /usr/sbin/nologin
Groups       : proxy

User         : www-data
Home folder  : /var/www
Start script : /usr/sbin/nologin
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /usr/sbin/nologin
Groups       : backup

User         : list
Home folder  : /var/list
Start script : /usr/sbin/nologin
Groups       : list

User         : irc
Home folder  : /var/run/ircd
Start script : /usr/sbin/nologin
Groups       : irc

User         : gnats
Home folder  : /var/lib/gnats
Start script : /usr/sbin/nologin
```

```
Groups        : gnats

User          : nobody
Ho [...]
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/08/05

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202409231210
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Ubuntu - 192.168.217.130
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.217.1
Port scanner(s) : netstat
Port range : default
Ping RTT : 14.289 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 : no
Credentialed checks : yes, as 'osboxes' 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 : 50
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/9/28 20:22 Egypt Standard Time
Scan duration : 177 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: 2024/07/24

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: 2024/07/24

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: 2024/07/24

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: 2024/07/24

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: 2024/07/24

Plugin Output

udp/38561

```
Port 38561/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: 2024/07/24

Plugin Output

udp/51234

```
Port 51234/udp was found to be open
```

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: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.4.0-84-generic on Ubuntu 18.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.4.0-84-generic on Ubuntu 18.04
```

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: 2024/09/03

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 osboxes 5.4.0-84-generic #94~18.04.1-Ubuntu SMP Thu Aug 26 23:17:46 UTC 2021 x86_64 x86_64
 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
buster/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 13.430744 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  : osboxes
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: 2024/09/18

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.6p1
Banner  : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
```

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.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2024/09/11

Plugin Output

tcp/0

```
Nessus detected 5 installs of OpenSSL:

  Path               : /usr/bin/openssl
  Version            : 1.1.1
  Associated Package : openssl 1.1.1-1ubuntu2.1
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Version            : 1.1.1
  Associated Package : libssl1.1

  Path               : /usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Version            : 1.1.1
  Associated Package : libssl1.1

  Path               : /usr/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.1.0.0
  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/lib4758cca.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libatalla.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/libnuron.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
```

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: 2024/09/10

Plugin Output

tcp/0

```
. You need to take the following 161 actions :

[ OpenSSH < 9.6 Multiple Vulnerabilities (187201) ]

+ Action to take : Upgrade to OpenSSH version 9.6 or later.

+Impact : Taking this action will resolve 3 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.

+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 / 23.10 / 24.04 LTS : LibTIFF
 vulnerability (USN-6827-1) (200307) ]

+ Action to take : Update the affected packages.
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio
 vulnerability (USN-6855-1) (201111) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less
 vulnerability (USN-6756-1) (194474) ]

+ Action to take : Update the affected less package.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerability
 (USN-6744-1) (193701) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities
 (USN-6891-1) (202187) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 41 different vulnerabilities (CVEs).



[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability
 (USN-6698-1) (192219) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server
 vulnerabilities (USN-6721-1) (192938) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).



[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulne [...]
```

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: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for 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 encryption_algorithms_server_to_client :

  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_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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 : osboxes
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
  Escalation method  : (none)
  Plugins :
  - Plugin Filename : bios_get_info_ssh.nasl
    Plugin ID       : 34098
    Plugin Name     : BIOS Info (SSH)
    - Command  : "LC_ALL=C dmidecode"
      Response : "# dmidecode 3.1\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
 Permission denied"
    - Command  : "LC_ALL=C /usr/sbin/dmidecode"
      Response : "# dmidecode 3.1\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
 Permission denied"
```

```
 - Plugin Filename : enumerate_aws_ami_nix.nasl
   Plugin ID       : 90191
   Plugin Name     : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
   - Command  : "/usr/sbin/dmidecode -s system-version 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
 - Plugin Filename : enumerate_oci_nix.nasl
   Plugin ID       : 154138
   Plugin Name     : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
   - Command  : "LC_ALL=C dmidecode -s chassis-asset-tag 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
   - Command  : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
     Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
Permission denied"
     Error    : ""
 - Plugin Filename : host_tag_nix.nbin
   Plugin ID       : 87414
   Plugin Name     : Host Tagging (Linux)
   - Command  : "sh -c \"echo 514953100729444997229426 1259cb56 > /etc/tenable_tag && echo OK\""
     Response : null
     Error    : "sh: 1: cannot create /etc/tenable_tag: Permission denied"
 - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
   Plugin ID       : 125216
   Plugin  [...]
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
SSH supported authentication : publickey,password
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2022/09/06

Plugin Output

tcp/0

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

  ii   accountsservice  0.6.45-1ubuntu1.3  amd64  query and manipulate user account information
  ii   acl  2.2.52-3build1  amd64  Access control list utilities
  ii   acpi-support  0.142  amd64  scripts for handling many ACPI events
  ii   acpid  1:2.0.28-1ubuntu1  amd64  Advanced Configuration and Power Interface event daemon
  ii   adduser  3.116ubuntu1  all  add and remove users and groups
  ii   adium-theme-ubuntu  0.3.4-0ubuntu4  all  Adium message style for Ubuntu
  ii   adwaita-icon-theme  3.28.0-1ubuntu1  all  default icon theme of GNOME (small subset)
  ii   aisleriot  1:3.22.5-1  amd64  GNOME solitaire card game collection
  ii   alsa-base  1.0.25+dfsg-0ubuntu5  all  ALSA driver configuration files
  ii   alsa-utils  1.1.3-1ubuntu1  amd64  Utilities for configuring and using ALSA
  ii   amd64-microcode  3.20191021.1+really3.20181128.1~ubuntu0.18.04.1  amd64  Processor microcode
 firmware for AMD CPUs
  ii   anacron  2.3-24  amd64  cron-like program that doesn't go by time
  ii   apg  2.2.3.dfsg.1-5  amd64  Automated Password Generator - Standalone version
  ii   app-install-data-partner  16.04  all  Application Installer (data files for partner
 applications/repositories)
  ii   apparmor  2.12-4ubuntu5.3  amd64  user-space parser utility for AppArmor
  ii   apport  2.20.9-0ubuntu7.29  all  automatically generate crash reports for debugging
  ii   apport-gtk  2.20.9-0ubuntu7.29  all  GTK+ frontend for the apport crash report system
  ii   apport-symptoms  0.20  all  symptom scripts for apport
```

```
ii   appstream  0.12.0-3ubuntu1  amd64  Software component metadata management
ii   apt  1.6.17  amd64  commandline package manager
ii   apt-config-icons  0.12.0-3ubuntu1  all  APT configuration snippet to enable icon downloads
ii   apt-utils  1.6.17  amd64  package management related utility programs
ii   aptdaemon  1.1.1+bzr982-0ubuntu19.5  all  transaction based package management service
ii   aptdaemon-data  1.1.1+bzr982-0ubu [...]
```

163103 - System Restart Required

Synopsis

The remote system has updates installed which require a reboot.

Description

Using the supplied credentials, Nessus was able to determine that the remote system has updates applied that require a reboot to take effect. Nessus has determined that the system has not been rebooted since these updates have been applied, and thus should be rebooted.

See Also

http://www.nessus.org/u?9e9ce1c1

http://www.nessus.org/u?fd8caec2

Solution

Restart the target system to ensure the updates are applied.

Risk Factor

None

Plugin Information

Published: 2022/07/14, Modified: 2023/11/27

Plugin Output

tcp/0

```
The following security patches require a reboot but have been installed since the most recent system
 boot:

The reboot required flag is set :

*** System restart required ***

The following packages require a reboot :

libc6
libssl1.0.0
dbus
linux-base
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User:       'osboxes'
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:       'osboxes'
Port:       22
Proto:      SSH
Method:     password
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot   system boot  5.4.0-84-generic Sat Sep 28 13:06   still running
reboot   system boot  5.4.0-84-generic Thu Sep 26 09:16 - 08:38  (-00:38)
reboot   system boot  5.4.0-84-generic Tue Sep 24 20:13 - 20:45  (00:31)
reboot   system boot  5.4.0-84-generic Mon Sep 20 07:46 - 07:47  (00:00)
reboot   system boot  5.4.0-84-generic Mon Sep 20 09:42 - 07:46  (-1:55)

wtmp begins Mon Sep 20 09:42:18 2021
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.217.1 to 192.168.217.130 :
192.168.217.1
192.168.217.130

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.182774' scanner setting in Nessus 8.15.1 or later.

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2024/09/11

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/bin/xz
  Version            : 5.2.2
  Associated Package : xz-utils 5.2.2-1.3ubuntu0.1
  Confidence         : High
```

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

    Path               : /lib/x86_64-linux-gnu/liblzma.so.5.2.2
    Version            : 5.2.2
    Associated Package : liblzma5 5.2.2-1.3ubuntu0.1
    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.

Original advisory details:

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 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: 2024/08/27

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 : xserver-common_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm8

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm8

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm8
```

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_1:7.6p1-4ubuntu0.7
```

```
  - Fixed package     : openssh-client_1:7.6p1-4ubuntu0.7+esm2

  - Installed package : openssh-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-server_1:7.6p1-4ubuntu0.7+esm2

  - Installed package : openssh-sftp-server_1:7.6p1-4ubuntu0.7
  - Fixed package     : openssh-sftp-server_1:7.6p1-4ubuntu0.7+esm2
```

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.

Original advisory details:

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs. An

attacker could possibly use this issue to cause the X Server to crash,

obtain sensitive information, or execute arbitrary code. (CVE-2023-6816)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

reattaching to a different master device. An attacker could use this issue

to cause the X Server to crash, leading to a denial of service, or possibly

execute arbitrary code. (CVE-2024-0229)

Olivier Fourdan and Donn Seeley discovered that the X.Org X Server

incorrectly labeled GLX PBuffers when used with SELinux. An attacker could

use this issue to cause the X Server to crash, leading to a denial of

service. (CVE-2024-0408)

Olivier Fourdan discovered that the X.Org X Server incorrectly handled

the curser code when used with SELinux. An attacker could use this issue to

cause the X Server to crash, leading to a denial of service.

(CVE-2024-0409)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

memory when processing the XISendDeviceHierarchyEvent API. An attacker

could possibly use this issue to cause the X Server to crash, or execute

arbitrary code. (CVE-2024-21885)

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled

devices being disabled. An attacker could possibly use this issue to cause

the X Server to crash, or execute arbitrary code. (CVE-2024-21886)

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

Note that Nessus has not tested for 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: 2024/08/27

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 : xserver-common_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-common_2:1.19.6-1ubuntu4.15+esm5

  - Installed package : xserver-xephyr_2:1.19.6-1ubuntu4.15
  - Fixed package     : xserver-xephyr_2:1.19.6-1ubuntu4.15+esm5

  - Installed package : xwayland_2:1.19.6-1ubuntu4.15
  - Fixed package     : xwayland_2:1.19.6-1ubuntu4.15+esm5
```

153569 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-5086-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5086-1 advisory.

Johan Almbladh discovered that the eBPF JIT implementation for IBM s390x systems in the Linux kernel miscompiled operations in some situations, allowing circumvention of the BPF verifier. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

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

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

See Also

https://ubuntu.com/security/notices/USN-5086-1

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF	USN:5086-1

Plugin Information

Published: 2021/09/22, Modified: 2024/08/27

Plugin Output

tcp/0

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

Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-86-generic
 for this advisory.
```

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.

Original advisory details: 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-6844-2

Solution

Update the affected packages.

Risk Factor

None

References

XREF	USN:6844-2

Plugin Information

Published: 2024/06/28, 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 : cups_2.2.7-1ubuntu2.10
  - Fixed package     : cups_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-bsd_2.2.7-1ubuntu2.10
  - Fixed package     : cups-bsd_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-client_2.2.7-1ubuntu2.10
  - Fixed package     : cups-client_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-common_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-core-drivers_2.2.7-1ubuntu2.10
  - Fixed package     : cups-core-drivers_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-daemon_2.2.7-1ubuntu2.10
  - Fixed package     : cups-daemon_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-ipp-utils_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ipp-utils_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-ppdc_2.2.7-1ubuntu2.10
  - Fixed package     : cups-ppdc_2.2.7-1ubuntu2.10+esm5

  - Installed package : cups-server-common_2.2.7-1ubuntu2.10
  - Fixed package     : cups-server-common_2.2.7-1ubuntu2.10+esm5

  - Installed package : libcups2_2.2.7-1ubuntu2.10
  - Fixed package     : libcups2_2.2.7-1ubuntu2.10+esm5

  - Installed package : libcupscgi1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupscgi1_2.2.7-1ubuntu2.10+esm5

  - Installed package : libcupsimage2_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsimage2_2.2.7-1ubuntu2.10+esm5

  - Installed package : libcupsmime1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsmime1_2.2.7-1ubuntu2.10+esm5

  - Installed package : libcupsppdc1_2.2.7-1ubuntu2.10
  - Fixed package     : libcupsppdc1_2.2.7-1ubuntu2.10+esm5
```

186358 - Ubuntu 18.04 ESM : poppler regression (USN-6508-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6508-2 advisory.

USN-6508-1 fixed vulnerabilities in poppler. The update introduced one minor regression in Ubuntu 18.04 LTS. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

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 this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6508-2

Solution

Update the affected packages.

Risk Factor

None

References

XREF USN:6508-2

Plugin Information

Published: 2023/11/28, 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 : libpoppler-glib8_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler-glib8_0.62.0-2ubuntu2.14+esm3

  - Installed package : libpoppler73_0.62.0-2ubuntu2.14
  - Fixed package     : libpoppler73_0.62.0-2ubuntu2.14+esm3

  - Installed package : poppler-utils_0.62.0-2ubuntu2.14
  - Fixed package     : poppler-utils_0.62.0-2ubuntu2.14+esm3
```

191054 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : OpenSSL update (USN-6663-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6663-1 advisory.

As a security improvement, OpenSSL will now return deterministic random bytes instead of an error when detecting wrong padding in PKCS#1 v1.5 RSA to prevent its use in possible Bleichenbacher timing 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-6663-1

Solution

Update the affected packages.

Risk Factor

None

References

XREF	USN:6663-1

Plugin Information

Published: 2024/02/27, 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 : libssl1.1_1.1.1-1ubuntu2.1~18.04.23
  - Fixed package     : libssl1.1_1.1.1-1ubuntu2.1~18.04.23+esm5

  - Installed package : openssl_1.1.1-1ubuntu2.1~18.04.23
```

```
  - Fixed package     : openssl_1.1.1-1ubuntu2.1~18.04.23+esm5
```

156710 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-5210-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5210-2 advisory.

USN-5210-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused failures to boot in environments with AMD Secure Encrypted Virtualization (SEV) enabled. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

Nadav Amit discovered that the hugetlb implementation in the Linux kernel

did not perform TLB flushes under certain conditions. A local attacker

could use this to leak or alter data from other processes that use huge

pages. (CVE-2021-4002)

It was discovered that the Linux kernel did not properly enforce certain

types of entries in the Secure Boot Forbidden Signature Database (aka dbx)

protection mechanism. An attacker could use this to bypass UEFI Secure Boot

restrictions. (CVE-2020-26541)

It was discovered that a race condition existed in the overlay file system

implementation in the Linux kernel. A local attacker could use this to

cause a denial of service (system crash). (CVE-2021-20321)

It was discovered that the NFC subsystem in the Linux kernel contained a

use-after-free vulnerability in its NFC Controller Interface (NCI)

implementation. A local attacker could possibly use this to cause a denial

of service (system crash) or execute arbitrary code. (CVE-2021-3760)

It was discovered that an integer overflow could be triggered in the eBPF

implementation in the Linux kernel when preallocating objects for stack

maps. A privileged local attacker could use this to cause a denial of

service or possibly execute arbitrary code. (CVE-2021-41864)

It was discovered that the KVM implementation for POWER8 processors in the

Linux kernel did not properly keep track if a wakeup event could be

resolved by a guest. An attacker in a guest VM could possibly use this to

cause a denial of service (host OS crash). (CVE-2021-43056)

It was discovered that the ISDN CAPI implementation in the Linux kernel

contained a race condition in certain situations that could trigger an

array out-of-bounds bug. A privileged local attacker could possibly use

this to cause a denial of service or execute arbitrary code.

(CVE-2021-43389)

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

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

See Also

https://ubuntu.com/security/notices/USN-5210-2

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF	USN:5210-2

Plugin Information

Published: 2022/01/13, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-94-generic
 for this advisory.
```

157458 - Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-5267-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5267-2 advisory.

USN-5267-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused the kernel to freeze when accessing CIFS shares in some situations.

This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

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 this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5267-2

Solution

Update the affected kernel package.

Risk Factor

None

References

XREF USN:5267-2

Plugin Information

Published: 2022/02/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
Running Kernel level of 5.4.0-84-generic does not meet the minimum fixed level of 5.4.0-99-generic
 for this advisory.
```

198218 - Ubuntu Pro Subscription Detection

Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

See Also

https://documentation.ubuntu.com/pro/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:

Binary Path                  : /var/lib/ubuntu-advantage
Binary Version               : 34~18.04
```

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  0.9  0.2 225768  9612 ?        Ss   13:06   0:09 /lib/systemd/systemd --system --
deserialize 41
root           2  0.0  0.0      0     0 ?        S    13:06   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   13:06   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   13:06   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   13:06   0:00 [kworker/0:0H-kb]
root           7  0.0  0.0      0     0 ?        I    13:06   0:00 [kworker/0:1-eve]
root           9  0.0  0.0      0     0 ?        I<   13:06   0:00 [mm_percpu_wq]
root          10  0.4  0.0      0     0 ?        S    13:06   0:04 [ksoftirqd/0]
root          11  0.0  0.0      0     0 ?        I    13:06   0:00 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    13:06   0:00 [migration/0]
root          13  0.0  0.0      0     0 ?        S    13:06   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    13:06   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    13:06   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    13:06   0:00 [idle_inject/1]
root          17  0.0  0.0      0     0 ?        S    13:06   0:00 [migration/1]
root          18  0.0  0.0      0     0 ?        S    13:06   0:00 [ksoftirqd/1]
root          20  0.0  0.0      0     0 ?        I<   13:06   0:00 [kworker/1:0H-kb]
root          21  0.0  0.0      0     0 ?        S    13:06   0:00 [kdevtmpfs]
root          22  0.0  0.0      0     0 ?        I<   13:06   0:00 [netns]
root          23  0.0  0.0      0     0 ?        S    13:06   0:00 [rcu_tasks_kthre]
root          24  0.0  0.0      0     0 ?        S    13:06   0:00 [kauditd]
root          26  0.0  0.0      0     0 ?        S    13:06   0:00 [khungtaskd]
root          27  0.0  0.0      0     0 ?        S    13:06   0:00 [oom_reaper]
root          28  0.0  0.0      0     0 ?        I<   13:06   0:00 [writeback]
root          29  0.0  0.0      0     [...]
```

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  : osboxes
Protocol : SSH
```

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

Synopsis

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

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2024/09/11

Plugin Output

tcp/0

```
Path    : /usr/bin/vmtoolsd
Version : 11.0.5
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

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: 2024/09/11

Plugin Output

tcp/0

```
Path    : /usr/bin/vim.tiny
Version : 8.0
```

198234 - gnome-shell Installed (Linux / UNIX)

Synopsis

gnome-shell is installed on the remote Linux / UNIX host.

Description

gnome-shell is installed on the remote Linux / UNIX host.

See Also

https://gitlab.gnome.org/GNOME/gnome-shell/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/31, Modified: 2024/09/11

Plugin Output

tcp/0

```
Path    : /usr/bin/gnome-shell
Version : 3.28.4
Managed : 1
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

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

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

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

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2024/09/11

Plugin Output

tcp/0

```
Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.5.0
Version            : 7.58.0
Associated Package : libcurl3-gnutls 7.58.0-2ubuntu3.24
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.182774' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2024/09/11

Plugin Output

tcp/0

```
Path               : /usr/lib/x86_64-linux-gnu/libexiv2.so.14.0.0
Version            : 0.25
Associated Package : libexiv2-14 0.25-3.1ubuntu0.18.04.11
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       : osboxes.local.
```